Symantec Brightmail™ Traffic Shaper 6.0 Implementation Guide

Symantec Brightmail™ Traffic Shaper Implementation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 6.0.1

Legal Notice

THIS DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID, SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043 USA

http://www.symantec.com

Technical support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's maintenance offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

For information about Symantec's Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/techsupp/

Contacting Technical Support

Customers with a current maintenance agreement may access Technical Support information at the following URL:

www.symantec.com/techsupp/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level

- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Select your country or language under Global Support.

Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and maintenance contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

If you want to contact Symantec regarding an existing maintenance agreement, please contact the maintenance agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Additional services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	These services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise Services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Chapter 3 Configuring Symantec Brightmail Traffic Shaper

Chapter 4 Working with Traffic Control

Chapter 5 Working with graphs and reports

Appendix A Example Deployment Scenarios

Appendix B Command Line Interface Reference

Introducing Symantec Brightmail Traffic Shaper

This chapter includes the following topics:

About Symantec Brightmail Traffic Shaper

The unique system design of Symantec Brightmail Traffic Shaper helps to reduce the amount of unwanted email entering enterprise networks by analyzing your network's email flow and identifying the behavior of various network paths over time.

Symantec Brightmail Traffic Shaper identifies spammers by pinpointing the true source of each email. Symantec Brightmail Traffic Shaper then limits the bandwidth and resources that spamming sources can use, significantly decreasing the flow of spam. It helps to prevent spam at its source, keeping it off your network and eliminating false positives.

Using Transmission Control Protocol (TCP) traffic shaping at the protocol level, the Symantec Brightmail Traffic Shaper manages the quality of service that each email sender is given based on how likely it is that they are sending spam. Legitimate senders receive excellent quality of service and their mail flows quickly, while spammers are given very poor quality of service and their mail is slowed dramatically. Spammers have no way to force mail into your protected network, so their spam simply backs up on their own servers.

The Control Center

Symantec Brightmail Traffic Shaper provides a secure, powerful Web-based administrative interface known as the Control Center. The Control Center lets you monitor, configure and administer your Symantec Brightmail Traffic Shaper installation.

Using the features of the Control Center you can:

- Monitor and manage the performance of your Symantec Brightmail Traffic Shaper installation
- Add, delete, and manage users of the Control Center
- Turn off and power down the Symantec Brightmail Traffic Shaper

Accessing the Control Center

Once you have completed setting up Symantec Brightmail Traffic Shaper as described in the next chapters, you can use your Web browser to access the Control Center.

The Control Center supports all HTML 4.0 compliant Web browsers, including:

- Microsoft Internet Explorer (version 6 or later)
- Netscape Navigator version (7 or later)
- Mozilla
- Firefox 1.0

Note: Symantec Brightmail Traffic Shaper uses a self-signed certificate to provide SSL security for the Web-based Control Center. You must accept this certificate to gain access to the Control Center.

Control Center permissions

The Control Center is a password-protected application that also lets administrators control the level of user access by assigning each user to one or more groups, which determines the functions that each user can perform.

Group name	Access
Help Administrator	Can view the path data and standard reports.
Path Administrator	Can view and modify the path data and view standard reports.
Data Administrator	Can view and modify both the path data and the reports.

Group name	Access
User Administrator	Can add, delete, and modify user accounts.
Master Administrator	Can perform any action, including changing configuration settings.
System Administrator	Can adjust the appliance state and power down the appliance.

Your user name can be assigned to one or more of the above groups, which determines the roles that are accessible to you in the Control Center.

What’s new in Symantec Brightmail Traffic Shaper

Table 1-1 lists the new and enhanced features.

Table 1-1 New features

Feature	Description
Outbound scanning for spam	Symantec Brightmail Traffic Shaper lets you scan your outbound mailflow for spam. See “Filtering outbound mail for spam” on page 60.

Chapter 2

Preparing to set up Symantec Brightmail Traffic Shaper

This chapter includes the following topics:

- Deployment Planning
- Operating modes and configuration considerations
- Placement considerations

Deployment Planning

The Deployment Overview provides a high level walkthrough of the process of integrating Symantec Brightmail Traffic Shaper into a network's mail stream at a high level.

The first thing to determine when planning Symantec Brightmail Traffic Shaper deployment is where email enters your network. Multiple physical sites may require multiple appliances, depending on where the mail systems that will be protected are located.

Next, consider the location within the network of the mail servers themselves. Symantec Brightmail Traffic Shaper is deployed on the network “upstream” of the mail servers to be protected. All inbound mail and the return traffic must flow through the appliance.

In order to accommodate a wide variety of network architectures, Symantec Brightmail Traffic Shaper can be installed as a Virtual Bridge (using proxy ARP), or a Router.

The Virtual Bridge deployment is the easiest to configure, as it generally does not require re-configuration of any upstream routers or the protected mail servers. It is best suited to networks where all protected mail servers reside on the same layer two network. As a Virtual Bridge, Symantec Brightmail Traffic Shaper is normally placed directly in front of the mail servers it is protecting, and all network traffic to and from those servers goes through the appliance. Details on deploying as a Virtual Bridge, including restrictions, are in “Virtual Bridge Mode” on page 19.

The Router deployment is better suited to networks where the protected mail servers are on different layer two networks, or the existing network architecture is too complex for the Virtual Bridge deployment. Details on deploying a simple Router configuration are in “Router Mode” on page 21.

Additional deployment scenarios, including using policy routing to direct only SMTP traffic through Symantec Brightmail Traffic Shaper, can be found in “Example Deployment Scenarios” on page 103.

To support high availability requirements, multiple Symantec Brightmail Traffic Shaper appliances can be deployed in a cluster. In a cluster, data is synchronized between appliances to insure the secondary (or backup) appliance is always up to date. A detailed discussion of high availability options for Symantec Brightmail Traffic Shaper is in “High availability and clustering” on page 22.

Installing the appliance

Installation of Symantec Brightmail Traffic Shaper is accomplished in two stages. At initial boot, you log on at the command line and are prompted for the basic information needed to get the appliance on the network. After the appliance is ‘bootstrapped’ onto the network, you use a Web browser to perform the remaining configuration using the browser-based Control Center.

Controlling traffic - Passthrough

When Symantec Brightmail Traffic Shaper is first installed, it comes up in Passthrough mode, where no traffic control is applied. In Passthrough mode, the appliance examines mail from source Paths (IP addresses), rating the mail as to the probability it is spam, and recording the results for each Path in the internal database.

Symantec Brightmail Traffic Shaper should be left in Passthrough for a minimum of 24 hours, but up to a week is recommended. This gives the appliance sufficient time to correctly learn about the Paths that regularly send mail to your network. The longer the time the appliance is in Passthrough, the more effective it will be when moved to 'Active' mode. Details on Traffic control can be found in "Working with Traffic Control" on page 59.

Controlling traffic – Active Mode

The final step in deploying Symantec Brightmail Traffic Shaper is moving the appliance from Passthrough to Active mode. In addition to examining mail and storing ratings just as Passthrough does, Active mode applies traffic control to all messages sent through it. Instructions for switching the appliance to Active mode are found in "Working with Traffic Control" on page 59.

There are five stages of Traffic Control shipped with Symantec Brightmail Traffic Shaper. Each stage more aggressively controls mail from spamming Paths. As with Passthrough mode, switching from stage to stage should be done in measured steps to allow Symantec Brightmail Traffic Shaper to continue to learn about your mail.

The following guidelines are recommended for the amount of time to stay in each Traffic control "stage."

Table 2-1 Traffic Control Guidelines

Stage	Minimal time	For a small mailstream	For a large mailstream
Passthrough	24hrs	5-7 days	3-5 days
Stage 1 - 5	24 hrs	3-5 days	1-3 days

Operating modes and configuration considerations

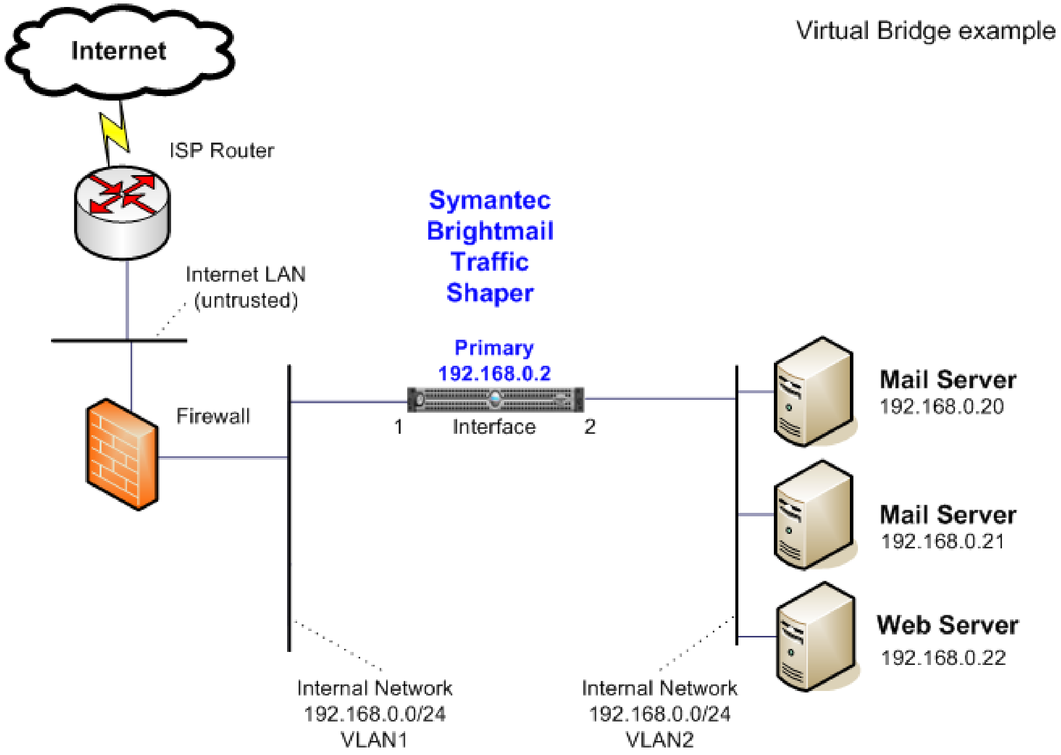
You can install Symantec Brightmail Traffic Shaper in one of two operating modes, depending on the characteristics of the network into which it is inserted. In addition to the diagrams in the following sections, refer to "Example Deployment Scenarios" on page 103 for other possible deployment options.

Virtual Bridge Mode

In Virtual Bridge mode, Symantec Brightmail Traffic Shaper appliances bridge traffic between parts of the same subnetwork. In this mode, you do not need to make any routing changes to the configuration of any devices upstream or downstream of Symantec Brightmail Traffic Shaper. Service interruptions for installation of bridge mode deployments are typically less than 10 minutes. This mode is recommended for simpler network architectures, where the flexibility of routed mode is not required. The internal and external interfaces must be on separate Layer 2 networks. In many networks, a VLAN is used to segment a switched network on a logical, rather than physical basis. You can insert a Symantec Brightmail Traffic Shaper into a network by linking VLANs.

Note: You cannot use Symantec Brightmail Traffic Shaper in Virtual Bridge mode in front of a router in a network using active routing protocols (such as OSPF).

Figure 2-1 Example of a Virtual Bridge implementation



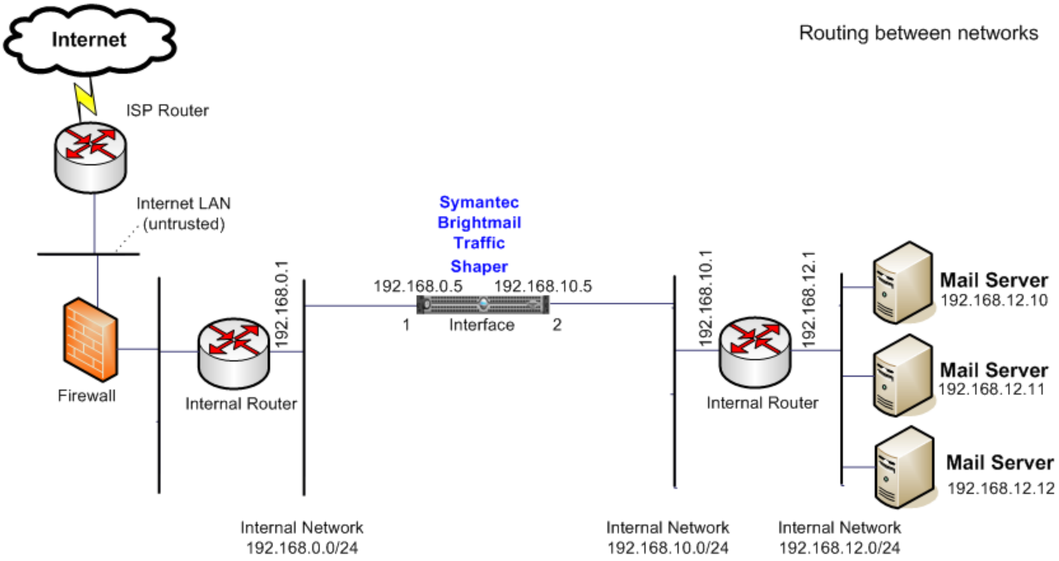
Router Mode

In Router mode, Symantec Brightmail Traffic Shaper appliances route traffic between two or more separate routed subnetworks. In this mode, you will most likely have to change gateways and routes both upstream and downstream of the appliance(s). This mode is recommended when the complexity of the protected network precludes bridging or if you want to perform outbound spam filtering.

See "Filtering outbound mail for spam" on page 60.

In Router mode, the return traffic must also be routed through the appliance. If your site passes a very high level of traffic, you may wish to implement a policy routed setup (such as the one described in "Policy routed router implementation" on page 107).

Figure 2-2 Example of a Router implementation



High availability and clustering

Symantec Brightmail Traffic Shaper appliances are reliable, robust devices capable of handling large volumes of traffic. However, in any environment where high availability is a key requirement, fault tolerance and redundancy is generally designed into the network architecture. It is generally recommended that you match the existing level of high availability in your protected email infrastructure when you deploy Symantec Brightmail Traffic Shaper.

Since Symantec Brightmail Traffic Shaper is a high throughput device, clustering for capacity purposes is needed only in the very largest of environments. More frequently, clustering is deployed to provide high availability. Active-passive clustering configurations serve this purpose.

The high availability feature uses the VRRP protocol to communicate availability between appliances.

To select a router configuration and implement high availability (using two Symantec Brightmail Traffic Shaper appliances):

- You must allocate the following IP addresses:
  - One IP address for each physical interface (four total)
  - One virtual IP address on the external network
  - The upstream devices (such as routers) direct mail to this IP address
  - One virtual IP address on the internal network
    The downstream devices (such as mail servers) direct return traffic to this IP address.
- You must also designate a virtual router ID (VRID) for the pair of appliances that is unique on the external subnet, including any other VRRP instances. The VRID must be a valid integer of value 1-254.

An example of a highly available router configuration is described in “High availability router implementation” on page 105.

To select a virtual bridge configuration and implement high availability, you must designate a virtual router ID (VRID) that is unique on the external subnetwork (including any other VRRP instances) for the pair of appliances. An example of a highly available virtual bridge configuration is described in “High availability virtual bridge implementation” on page 104.

Bridged active-passive

Bridged configurations implement active-passive clustering by virtualizing the bridging responsibility across the two cluster members. In the event of a component failure, bridging responsibility is immediately transferred to another cluster member, and all appropriate ARP entries on network peers are updated. The transfer of bridging responsibility is transparent to existing sessions.

Routed active-passive

Routed configurations implement active-passive clustering by virtualizing gateway addresses on all networks across the two cluster members. In the event of a component failure, the gateway addresses are immediately transferred to another cluster member, and all appropriate ARP entries on network peers are updated. The transfer of gateway addresses is transparent to existing sessions.

MX active-active

Most large environments have primary and secondary MXs in different physical locations. MX active-active clustering places a Symantec Brightmail Traffic Shaper in front of each MX, protecting the network from spam traffic while using the existing multiple MX implementation high availability. This is accomplished using the Data Synchronization feature described in "Synchronizing data between appliances" on page 52.

Unless high availability strategies within each physical location require additional clustering, MX active-active with a distributed cluster made up of one cluster member per physical location can be used.

Data Synchronization

The Symantec Brightmail Traffic Shaper can also synchronize network path information between appliances. This is used to keep appliances in a local high availability installation up to date as well as distributed clusters such as an MX-MX active deployment.

Advanced Failover

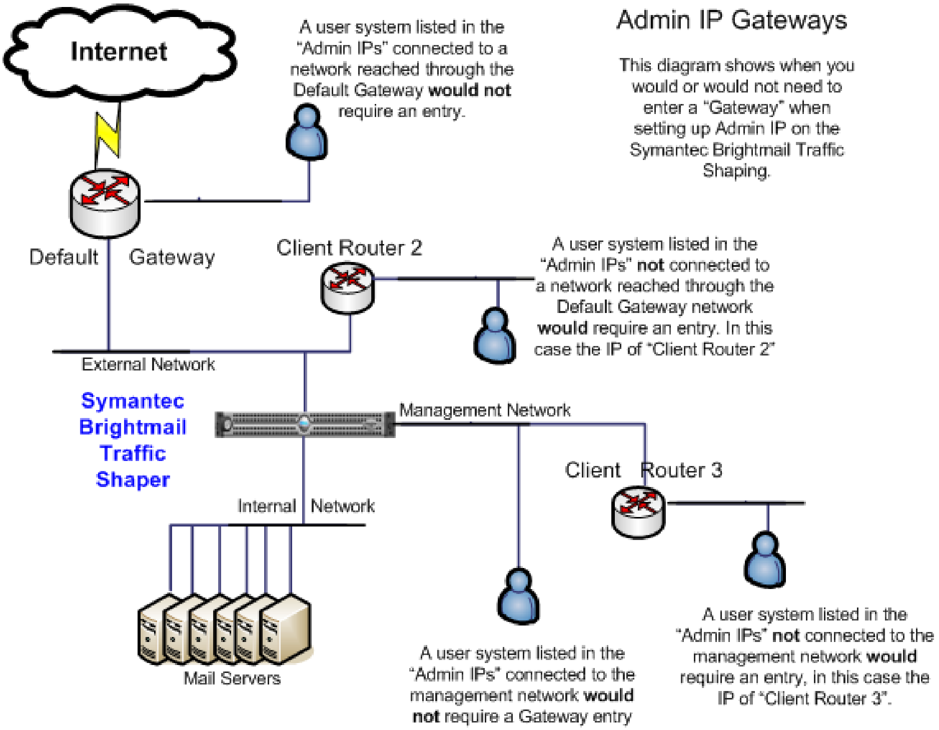
The Advanced Failover feature of Symantec Brightmail Traffic Shaper allows the appliance to participate as a primary or backup device in a cluster of up to four appliances. It is intended to offer a high level of redundancy in dual-homed, policy routed configurations For more information about advanced failover, refer to "About advanced failover" on page 53.

Management network interface considerations (optional)

An optional third network interface is available for Symantec Brightmail Traffic Shaper. You can specify that all HTTPS, SSH, and SNMP protocol connections be restricted to this interface, and additionally specify CIDR blocks from which access is allowed to the Control Center, command line interface and the SNMP server.

If you configure a management network interface and you have restricted HTTPS, SSH, and SNMP protocol connections to it, then you must set a Gateway IP address on the network the management interface is attached to for each CIDR to properly route this traffic back to its source.

Figure 2-3 Management network interface gateway requirements



Internet
A user system listed in the "Admin IPs" connected to a network reached through the Default Gateway **would not** require an entry.
Admin IP Gateways
This diagram shows when you would or would not need to enter a "Gateway" when setting up Admin IP on the Symantec Brightmail Traffic Shaping.
Default Gateway
Client Router 2
A user system listed in the "Admin IPs" **not** connected to a network reached through the Default Gateway network **would** require an entry. In this case the IP of "Client Router 2"
External Network
Symantec Brightmail Traffic Shaper
Management Network
Client Router 3
Internal Network
Mail Servers
A user system listed in the "Admin IPs" connected to the management network **would not** require a Gateway entry
A user system listed in the "Admin IPs" **not** connected to the management network **would** require an entry, in this case the IP of "Client Router 3".

Placement considerations

As a device, the essential role of Symantec Brightmail Traffic Shaper is to act as a router or a virtual bridge in a network. As such, it should be placed into the network at a point upstream of the email infrastructure. The portion of the network downstream of Symantec Brightmail Traffic Shaper is known as the "protected network."

You can place Symantec Brightmail Traffic Shaper inside or outside firewalls and in front of all types of network traffic; all non-email traffic passing through the appliance is forwarded without any inspection or control.

Keep the following in mind:

- Access to the original TCP session between the Internet and the protected mail servers (including non-NAT-ed source addresses) is required in order to control resource allocation. Destination NAT, however, is acceptable.
- Do not deploy a load balancer in front of multiple instances of Symantec Brightmail Traffic Shaper. Load balancers for your mail servers behind Symantec Brightmail Traffic Shaper are acceptable.
- You cannot use Symantec Brightmail Traffic Shaper in Virtual Bridge mode in front of a router in a network using active routing protocols (such as OSPF).
- In Router mode you must ensure the return traffic is also routed through the appliance.

Installing in multiple locations

If your email network has several entry points (either physical or logical), you may wish to install a Symantec Brightmail Traffic Shaper to protect each individual physical or logical entry point. Commonly, most email infrastructure deployments include multiple email servers. A single Symantec Brightmail Traffic Shaper can protect a large cluster of email servers – some installations protect hundreds of email servers. In situations where high availability and failover is required, you can deploy Symantec Brightmail Traffic Shaper appliances in clusters. The important points to remember are to place the Symantec Brightmail Traffic Shaper upstream of the email infrastructure (often before the first gateway MTA server), and that in most cases, multiple entry points into the networks email servers are protected by multiple appliances. You may wish to use the Advanced failover features described in "Advanced Failover" on page 23.

Firewall considerations

Generally, you should place Symantec Brightmail Traffic Shaper behind the firewall. However, you cannot place Symantec Brightmail Traffic Shaper behind firewalls that implement full store-and-forward SMTP proxies. You should also not place the appliance behind full TCP proxies. Access to the original TCP session between the Internet and the protected mail servers (including non-NAT-ed source addresses) is required in order to control TCP resource allocation.

You can use a full-TCP proxy firewall, but you must disable the proxy for the SMTP port. Consult your firewall documentation for details.

Port access requirements

All Symantec Brightmail Traffic Shaper appliances need access to the Symantec central servers for software and security updates.

In addition:

- TCP/ 22 (SSH) for access to aztec.brightmail.com for software updates

  If multiple Symantec Brightmail Traffic Shaper appliances are deployed in a cluster, bidirectional access to TCP/22 is required for all members of the cluster to support data synchronization within the cluster.
- HTTP/80 (HTTP) for management access
- Local TCP/53 and/or UDP/53 for access to local DNS servers
- TCP/112 (VRRP) if High Availability is enabled
- TCP/123 access for NTP servers
- TCP/161 (SNMP) if SNMP is enabled
- TCP/443 must be allowed for the following access:
  - Control Center (the Web-based administration interface)
  - Symantec Licensing server
  - aztec.brightmail.com for software updates

Addressing for high availability implementations

For a Virtual Bridge configuration, you must allocate the following IP addresses:

- One IP address for each physical appliance (two total)
- The upstream devices (such as routers) direct mail to the IP address of the mail server(s) on the protected network
- The downstream devices (such as mail servers) direct return traffic to the same gateway device IP address they did before Symantec Brightmail Traffic Shaper was put in place

For a router configuration, you must allocate the following IP addresses:

- One IP address for each physical interface (four total)
- One virtual IP address on the external network
  The upstream devices (such as routers) direct mail to this IP address.
- One virtual IP address on the internal network
  The downstream devices (such as mail servers) direct return traffic to this IP address.

You must also designate a virtual router ID (VRID) that is unique on the external subnetwork (including any other VRRP instances) for the pair of appliances. An example of a high available router configuration is described in "High availability virtual bridge implementation" on page 104.

Note: It may be helpful for you to make a list of every single physical and virtual address on the layer 3 network that will be located behind Symantec Brightmail Traffic Shaper as you will have to designate each of them as a protected server. Do not include IPs that are on the external (not-protected) network, or portions of your network may become unreachable.

Security considerations

Symantec Brightmail Traffic Shaper was designed from the ground up to meet the stringent security requirements of the networks in which it is deployed. The appliance incorporates a stateful inspection firewall primarily to protect itself from outside attack. Access to the appliance is encrypted at all times, and is authenticated using multiple factors.

Chapter 3

Configuring Symantec Brightmail Traffic Shaper

This chapter includes the following topics:

Installation and deployment time

Installation and deployment of Symantec Brightmail Traffic Shaper ranges in complexity from that of adding a transparent network component to the existing environment (Virtual Bridge Mode) to that of adding a router and additional subnetworks to the existing environment (Router Mode). Most deployments use the Virtual Bridge Mode, and are extremely straightforward. Virtual Bridge Mode deployments are typically completed with less than 10 minutes of service interruption to the email environment.

Before you begin

Note: If you are using the optional fiber-optic interface, refer to the specialized setup documentation for that interface. The procedures in this document do not apply.

To install Symantec Brightmail Traffic Shaper, you will need the following information:

For Virtual Bridge mode:

- Valid license file from Symantec
- Hostname
- IP address, netmask, and default gateway for the appliance (in Virtual Bridge mode, only 1 IP per appliance is needed)
- If implementing a high availability cluster at the same location:
  - IP address for the second appliance
  - Virtual Router ID (VRID) for the appliances (a valid integer of value 1-254, shared by all appliances in the same cluster)
- Domain Name servers (DNS)
- NTP Servers (optional)
- List of protected servers
- IP address and port for HTTP proxy (optional)
- IP address and netmask for Management NIC (optional)
- IP addresses from which to allow management traffic (optional)

For Routed mode:

- Valid license file from Symantec
- Hostname
- IP address and netmask for the external interface
- IP address and netmask for the internal Interface
- Default gateway
- If implementing a high availability cluster as the same location:
  - IP address and netmask for the external interface for the second appliance
  - IP address and netmask for the internal interface for the second appliance

  - Virtual IP and netmask for the external interface
    This is the IP address to which inbound mail is sent.
  - Virtual IP and netmask for the internal interface
    This is the IP address to which return traffic is sent.
  - VRID for the appliances (a valid integer of value 1-254, shared by all appliances in the same cluster)
- Domain Name servers (DNS)
- NTP Servers (optional)
- List of protected servers
- IP address and port for HTTP proxy (optional)
- IP address and netmask for Management NIC (optional)
- IP addresses from which to allow management traffic (optional)

About configuring Symantec Brightmail Traffic Shaper

To configure a new Symantec Brightmail Traffic Shaper, you must do the following:

- Plug in, power up, and initialize the appliance.
  See "Initializing Symantec Brightmail Traffic Shaper" on page 32.
- Register the appliance.
  See "Registering your appliance" on page 34.
- Run the Setup Wizard to configure the network and other appliance settings.
  See "Setting up your appliance" on page 35.

Identifying the network adaptors

When looking at the rear of the appliance, `eth0`, the connector you should use to connect to your external network, is labeled 1, and `eth1`, the connector you should use for your internal network, is labeled 2. If you have installed the optional Management network card, it will be in PCI slot 2.

Warning: YOU **MUST** FULLY CONFIGURE THE SYSTEM BEFORE IT WILL BRIDGE TRAFFIC. CONNECT THE EXTERNAL INTERFACE (LABELED INTERFACE 1) TO THE NETWORK BUT **DO NOT** PLUG IN THE INTERNAL INTERFACE (LABELED INTERFACE 2) UNTIL YOU HAVE SUCCESSFULLY COMPLETED CONFIGURATION.

Initializing Symantec Brightmail Traffic Shaper

When you first power up your appliance, you will perform a one-time initialization sequence to get it up and running.

To initialize your new appliance

1. Unpack the appliance and either rackmount it or place it on a level surface.
2. Plug in AC power.
3. Connect a keyboard and VGA monitor to the appliance or connect a serial console cable to the serial port on the back of the device.
   If using a serial console, the line settings are 9600 baud, 8 data bits, 1 stop bit and no parity.
4. Connect an ethernet cable to the external (eth0, interface 1) interface jack on the back panel.
   When looking at the rear of the appliance, `eth0`, the connector you should use to connect to your external network, is labeled 1, and `eth1`, the connector you should use for your internal network, is labeled 2. If you have installed the optional Management network card, it will be in PCI slot 2.
   If you intend to use the appliance for outbound scanning, connect the external network to eth1 and the internal network to eth0.
   See “Filtering outbound mail for spam” on page 60.
5. Switch on the power.
   The appliance will boot up.
6. Log in on the console and change your password.
   The starting login information is:
   - username: **admin**
   - password: **symantec**
7. Type your new password twice when prompted.
   You are next asked for the host name.

8 Type a fully qualified name for this host.

For example:

`hosta.companyb.com`

Next, you will be asked to supply the IP address for the Ethernet port labelled **1** on the back of the appliance. When looking at the back of the appliance, it is the connector on the right hand side. This port corresponds to the `eth0` network interface.

9 Enter the IP address for the external network interface,`eth0`, for this appliance. For example:

```
192.168.0.1
```

You are asked for network addressing information.

10 Enter the additional network information for this appliance when prompted (netmask and default gateway).

11 Choose to set up the default gateway on an external or internal interface. The default choice is external.

The interface will default to the correct values for the broadcast and network addresses.

If you have installed a third network interface card for management-only access, you will be prompted for the IP address and netmask of the management interface. If not, skip to step 14.

12 Enter the network information for the optional management network interface when prompted.

You are asked if you want to restrict access to the management protocols on the appliance (HTTPS, SSH, SNMP) to connections originating **only** on the management network interface.

13 Type **Y** if you wish to restrict access or **N** if you do not.

You are then asked if you want to restrict access to the management protocols on the appliance (HTTPS, SSH, SNMP) to connections originating from certain CIDRs that you specify.

14 Do one of the following:

- Enter an initial CIDR and gateway from which to allow connections so that you can complete setting up this appliance using the Control Center. You can specify additional CIDRs at that time.
- Enter **none** if you do not want to restrict management access to the appliance at this time.

15 Enter the nameserver for this appliance.

16 If you are using an HTTP proxy server, you *must* provide the IP address and port at this time; there is no option to provide this information later.

If the appliance has direct access to the internet for HTTP/HTTPS connections, leave this set to none.

17 Choose the Timezone for your appliance, and type **Y**.

18 Enter the Date and Time for the appliance.

19 If the summary information is correct, type **Y**, if not type **N** and make changes.

The appliance will reboot. Once it has finished, continue with the next procedure, "Registering your appliance" on page 34.

Registering your appliance

After you complete the initialization process, you must log into the Control Center using the password you set during initialization in order to register the appliance. You can access the appliance from any computer that can connect to the appliance using a Web browser.

Note: Your appliance must have outbound 443 connectivity or connectivity via an HTTP proxy in order for activation/registration to succeed.

To complete registration, you will need the license file (.slf file) you received via email from Symantec when you registered your license entitlement. Place this file on the computer from which you are accessing the Control Center.

To register your appliance

1 From a computer that can access the new appliance, log into the appliance using a browser.

The default login address is:

https://`<IP-address>`

where **`<IP-address>`** is the IP address you designated for your appliance during initialization. The default port, which you do not need to enter, is 443.

Accept the self-signed SSL certificate.

The Control Center log in page is displayed.

2 Log in as user **admin**, using the password you set during initialization.

The Appliance Registration page is displayed, showing the license status of each feature.

3 On the Licensing page, select the **From a file on my computer** radio button, then click **Browse** to find your .slf file.

If you have other Symantec license files, be sure you select the correct one.

4 Select your `.slf` file and click **Open** to return to the Licensing page.

5 Click **Install**.

- If registration was successful, the Appliance Registration page is redisplayed.
- If there was an error, you will see error text at the top of the page; visit Symantec's support Web site for assistance. Check to make sure the appliance you are registering has net connectivity. Log into the command line interface and ping an outside network site by its domain name. If you do not have connectivity from the appliance, you may have mis-configured the IP or gateway address during initialization. If this is the case, you may wish to repeat the initialization procedure. To do this, log in to the console as user **admin**, and from the command line, type:

```
bootstrap --reconfigure
```

and proceed through the initialization process described in "Initializing Symantec Brightmail Traffic Shaper" on page 32.

6 When your `.slf` file is successfully registered, click **Next** to proceed to the Software Update Page.

7 Do one of the following:

To update your software	Click **Update**. The appliance will reboot. The next time you log in, the Setup Wizard will be displayed.
No software updates are available or you do not want to update the software at this time	Click **Next**. The setup mode proceeds without rebooting.

8 Proceed to the next section, "Setting up your appliance" on page 35.

Setting up your appliance

In order for Symantec Brightmail Traffic Shaper to begin traffic-shaping, you must provide it with information about where it is in your network infrastructure, and about how to direct network traffic.

Warning: Do not plug the internal (interface labeled 2) interface jack into the network until you have successfully completed setting up the appliance.

Warning: Until you have activated the configuration, Symantec Brightmail Traffic Shaper will not bridge or route traffic to the protected network. Placing your mail servers on the protected network before you are ready to activate a configuration will cause an interruption in service.

Warning: Defining protected servers in Bridge mode will cause Symantec Brightmail Traffic Shaper to start ARPing for those devices immediately, so if they already exist on the unprotected network there will be address collisions.

Before you configure

The first time you log into the Control Center after initializing and registering the appliance, the Setup Wizard runs, allowing you to configure your appliance. Navigate back and forth within the pages of the wizard using the **Save & Continue** and **Back** buttons at the bottom of each page. Do not use the Forward and Back buttons of your browser.

To reach the Setup Wizard again in the future, log into the Control Center, click Settings at the top of the page, and choose Edit Settings from the left hand menu. To confirm and activate new settings, you must click Go to Activation and then click Activate, which will reboot the appliance and apply the new settings.

When you edit the settings on an appliance, but have not yet clicked Activate, the Settings tab will display an asterisk (*) to let you know that you have not yet activated the changes you made. You can cancel on any page, or clear your changes by reverting to previous settings. For more information about reverting settings, refer to "Reverting settings" on page 51.

Note: With the exception of the Set Time Now function, no configurations changes will take effect until you complete the wizard and click Activate on the last page.

Configuring Symantec Brightmail Traffic Shaper

The following procedures describe how to set up two Symantec Brightmail Traffic Shaper appliances in a high availability configuration as either a virtual bridge or as a router. If you are installing a single appliance, you can skip the high availability steps.

If you have multiple Symantec Brightmail Traffic Shaper appliances to set up, you may wish to refer to "Configuring multiple appliances" on page 49 for options.

To configure Symantec Brightmail Traffic Shaper, log into the Control Center, click Settings at the top of the page, and choose Edit Settings from the left hand menu. If this is the first time you are configuring this appliance, the Setup Wizard runs automatically.

If you are making changes to an existing configuration option, you can access its panel directly from the left hand menu, and then click Go to Activation when you are finished making changes.

◆ To begin, click **Save & Continue**.

Note: You can use the following hot keys to navigate through the Setup Wizard:

`Alt+B` to move back one page

`Alt+N` to move forward one page

These hotkeys are browser independent, and are only active in the Setup Wizard, not in any other portion of the Control Center.

To set up DNS, time, and proxy settings

The first panel of the Setup Wizard is the DNS Setup panel. The values you entered during the initialization process are entered by default.

1. Specify up to three domain name system (DNS) servers to use.
   You must use IP addresses to specify the DNS Servers, not hostnames. Symantec Brightmail Traffic Shaper will use these DNS servers to perform DNS lookups.
2. If you wish, change the hostname of your appliance.
3. Click **Save & Continue**.
   The Time Settings panel is displayed.
4. On the Time Settings panel, specify your system-wide time settings.
   You can change the timezone from what was specified during initialization, reset the date and time on the appliance, and configure the system to use NTP.
   Two NTP servers are configured by default. You can use these, replace them with ones of your choice, or disable NTP by deleting all of the entries.

Note: As mentioned at the beginning of the Setup Wizard procedure, if you click the **Change time settings now** button, the system timezone and time are set on your appliance immediately; you do not have to proceed to the Settings Activation panel and confirm before this setting takes effect.

5 Three NTP servers are configured by default. You can use these, replace them with ones of your choice, or disable NTP by deleting all of the entries.

6 Click **Save & Continue**.
The Proxy Settings panel is displayed.
On this panel, you can specify an HTTP proxy for the appliance to use.

7 (optional) Click the **Enable proxy settings** checkbox, then enter the hostname and port, and click **Save & Continue**.

To choose virtual bridge or routed configuration

The Bridged vs. Routed panel is displayed.

Depending on the requirements of your network infrastructure, you can specify that Symantec Brightmail Traffic Shaper act as a virtual bridge or as a router.

Note: You cannot use Symantec Brightmail Traffic Shaper in bridged mode in front of a router in a network using active routing protocols (such as OSPF).

1 Choose a configuration from the Configuration Type panel:

- If you want to configure Symantec Brightmail Traffic Shaper as a virtual bridge, choose **Bridged Configuration**.
- If you want to configure Symantec Brightmail Traffic Shaper as a router, choose **Routed Configuration.**

If you wish to configure your Symantec Brightmail Traffic Shaper installation for high availability, you must have two appliances in the same location. You will designate one as the primary appliance, and one as the secondary appliance. The primary appliance will synchronize data to the secondary appliance.

2 If you are configuring a single Symantec Brightmail Traffic Shaper appliance and will not add a second for high availability in the same location, skip to the next section.

Note: If you select a router configuration, you must allocate a third IP address to use as a virtual IP for both appliances (in addition to the IP each appliance has on the real network.

If you chose a Routed Configuration and have more than two Symantec Brightmail Traffic Shaper appliances in the cluster, you may want to set up advanced failover. For more information about advanced failover, refer to "About advanced failover" on page 53.

3 From the High Availability panel, specify whether this is the primary or secondary appliance.

4 Click **Save & Continue**.

To set up interfaces

The Configuration Setup panel is displayed.

1 Enter configuration information:

- If this is a Virtual Bridge configuration, enter the IP address, and netmask for the interfaces.
- If this is a Routed configuration, enter the IP address, and netmask for the pair of interfaces.
- If you have installed an optional management network interface card, enter the IP address and netmask for this IP.

2 For each interface, select **Auto** to tell the appliance to auto-negotiate with the switch, or **Lock** if you would like to specify a rate.
If you choose **Lock**, you must also choose half or full duplex and set a speed.

Note: Symantec recommends against auto-negotiation.

3 If you chose **Lock** for one or both interfaces, select full or half duplex, and a speed of 10/100/1000 gigabits.

Note: Make sure you set the speed correctly for your network. The most common cause of intermittent network problems is misconfigured network speed and duplex problems, as many common networking products do not auto-negotiate properly.

4 If you want to use a different port than the default port of 25, type the port number you want to use in the **SMTP Port** field.

5 If you designated this appliance as participating in failover, in the Failover box, specify the internal and external virtual IP addresses (applies to Routed configurations only) and the virtual router ID.

6 Click **Save & Continue**.

To specify management access

The Management Access panel is displayed.

On this panel, you can specify CIDR blocks from which access is allowed to the Control Center, command line interface and the SNMP server. Entries will automatically be added for any Data Synchronization peers defined.

You can specify allowed blocks one at a time, or upload a file containing one CIDR block per line.

Note: If no CIDR blocks are specified, no IP based restrictions will be enforced on remote access.

You can restrict incoming HTTPS, SSH, and SNMP connections to the Management network interface only.

You can also enable a customizable block of text that is displayed to all users of the system when they log into the Control Center.

1 (optional) Only if you have a third Management NIC, you can restrict HTTPS, SSH, and SNMP protocol access so that connections are allowed over the Management network interface only. To do so, select the appropriate radio button in the **Restrict Access** box.

2 To add allowed CIDR blocks, do one of the following:

- Enter a CIDR block into the **CIDR block:** field and click **Add Access**. Enter an optional Gateway IP to reach the CIDR. If you have restricted HTTPS, SSH, and SNMP protocol connections to the Management network interface, then you must set a Gateway IP address on the network the management interface is attached to for each CIDR to properly route this traffic back to its source. Refer to “Management network interface considerations (optional)” on page 24 for more information.
- Enter the path to a file containing the list of allowed CIDR blocks and optional Gateway IP address into the **Access List Upload** field or browse for the file, and click **Upload Access List**.

  The file format is: **`CIDR[,Gateway]`**

  The file containing the list must be browsable from the machine you are currently using to access the Control Center.

  The allowed blocks are displayed in the **Management Access list**.

3 To remove a block’s access, select it from the Management Access list and click **Remove Access**.

4 To enable the customizable logon disclaimer, check the **Logon Disclaimer** checkbox.

The logon disclaimer field is activated. You can enter up to 1024 characters of text which will be displayed to all users as they log into the Control Center.

5 Enter the text you want displayed to all users as they log in.

6 Click **Save & Continue**.

To set up network routes and protected servers

The Routes panel is displayed.

1 Specify routes here to be added to the routing table for special network situations.

2 Click **Save & Continue**.

The Protected Servers panel is displayed.

3 Add the IP addresses and gateway for any systems that are on the LAN behind Symantec Brightmail Traffic Shaper.

- For a virtual bridge configuration, you must add every host behind the appliance. This includes non-mail traffic. Hosts on the protected network that are not in the Protected servers list will not be accessible from the external network.
- For a routed configuration, you must also add the next-hop gateway to each protected host.
- You *must* place the protected server on the network behind Symantec Brightmail Traffic Shaper before activating the configuration at the end of the Setup Wizard.

Note: ARP cache issues

In virtual bridge mode, Symantec Brightmail Traffic Shaper responds to ARP requests from upstream devices for all protected servers with the MAC address of interface one. When a protected server is defined in Symantec Brightmail Traffic Shaper, the appliance will issue gratuitous ARPs "announcing" the change in MAC address for the protected server. If an upstream device (such as a router) has a long ARP cache timeout value, it may not recognize that the MAC address changed for a protected server and attempt to forward mail to the mail system instead of Symantec Brightmail

Traffic Shaper. In this case, all affected upstream devices should have the protected server's entry flushed from their ARP caches.

Similarly, Symantec Brightmail Traffic Shaper responds to ARP requests from protected servers for upstream devices with the MAC address of interface two. The appliance will issue gratuitous ARPs "announcing" the change in MAC address for any upstream device to the protected servers. If a protected server has a long ARP cache timeout value, it may not recognize that the MAC address changed for an upstream device and attempt to forward mail to the device instead of Symantec Brightmail Traffic Shaper. In this case, all affected mail servers should have the upstream device's entry flushed from their ARP caches.

If there is an intermediary router between the appliance and the mail servers, the next-hop gateway is the IP address of the router. If there is no intermediary router between the appliance and the mail servers, then the next-hop gateway should be set to 0.0.0.0. Refer to the High availability router implementation and Mail server gateway router implementation examples in "Example Deployment Scenarios" on page 103.

If you have a large list of hosts to enter, you can upload them through the browser.

- For a virtual bridge configuration, the file format is a plain text file consisting of one IP address per line.

  For example:

  ```
  192.168.3.3
  192.168.3.4
  ```

- For a routed configuration, the file format is a plain text file, each line consisting of the protected server IP address, a comma, and the next hop gateway address.

  For example:

  ```
  192.168.3.3,192.168.3.254
  192.168.3.4,192.168.3.254
  192.168.3.4,192.0.0.0.0
  ```

4 Click **Save & Continue**.

To set up outbound paths, exempt IPs, and connection shaping

The Outbound paths panel is displayed.

1 Use the Outbound paths panel to specify outbound CIDR blocks for which Symantec Brightmail Traffic Shaper will control traffic.

If you are specifying paths that are assigned by DHCP for a number of individual users, perhaps by means of a modem pool, you can set a refresh rate in minutes for Symantec Brightmail Traffic Shaper to use to purge the history it has acquired for these paths. Most likely, you will want to set the refresh rate so that it matches the DHCP lease time.

If you have a large list of outbound paths to enter, you can upload a plain text file, with one IP address per line. For example:

```
192.168.3.3
192.168.3.4
```

2 If you are specifying paths that are assigned by DHCP for a number of individual users, perhaps by means of a modem pool, you can set a refresh rate in minutes for the Traffic Shaper to use to purge the history it has acquired for these paths. Most likely, you will want to set the refresh rate so that it matches the DHCP lease time.

3 If you have a large list of outbound paths to enter, you can upload a plain text file that contains one IP address per line.

4 Click **Save & Continue**.

The Exempt IP panel is displayed.

An exempt IP address is a destination address for a host or CIDR block behind Symantec Brightmail Traffic Shaper for which you do not wish to control SMTP traffic. In contrast, a whitelisted IP address is a *source* address for which you do not wish to control traffic. To whitelist an address or block of addresses, refer to "Uploading whitelisted or blacklisted paths in bulk" on page 89.

Traffic to IPs you provide on the Exempt IPs panel will pass through Symantec Brightmail Traffic Shaper without any lookup or processing, as opposed to IPs you add to the whitelist, which are still looked up and logged before passing through.

5 Add any networks you wish to exempt from processing.

To exempt a single host, add it with a CIDR value of /32.

6 Click **Save & Continue**.

The Connection Shaping panel is displayed.

On this panel, you can specify some options for traffic shaping.

- Earlytalk -- You can choose to terminate SMTP connections with any client that attempts to send data before your mail server indicates readiness. The SMTP standards specify that sending hosts must wait for certain events to occur in the SMTP session before message commands can be issued. A number of malware programs, viruses and spam delivery products often do not obey these rules, and therefore emit commands and data strings prematurely. This "earlytalk" is a very good indicator of sending hosts which will attempt to deliver unwanted email. Checking this box causes Symantec Brightmail Traffic Shaper to immediately terminate any connections which exhibit this behavior.

- Rejection Characteristics -- You can designate the rejection characteristics that Symantec Brightmail Traffic Shaper uses when there are no more connections available for blacklisted or regular paths. Choose from TCP RST or SMTP error, or to drop the connection silently (this option is only available for blacklisted paths). TCP RST sends a TCP reset and drops the connection. SMTP Error sends an SMTP error message and drops the connection. You can customize the SMTP error number and text, using the fields under SMTP Return Codes. To activate the Reject field, choose SMTP Error for Blacklist. To activate the Defer field, choose SMTP Error for All Others. You must enter a three-digit number followed by a space and text characters. To return to the default texts, clear the fields and click Save & Continue.
- Bounced NDR detection -- You can enable the detection of double bounce NDRs (non-delivery reports). If a valid mail server bounces a spam message and includes the full contents of that spam message in the NDR, that mail server may be labeled as a source of spam. If you enable this setting, NDRs containing full spam messages will not cause the Spam Reputation for the remote mail server's IP address to be incremented.
- Enable BRS data -- You can enable the use of Brightmail Reputation Service data, which includes dynamically updated lists of known 'zombie' IPs, suspect IP addresses that send mostly spam, and safe IP addresses that rarely send spam.

7 Make your selections and click **Save & Continue**.

To specify antispam settings

1 Specify the rule set that you want to use as follows:

Full rule set	This rule set provides the following features: ■ Includes the predictive rules for spam detection ■ Provides more effectiveness for certain types of spam attacks ■ Requires more CPU resources ■ Results in a low, false positive rate This is the default setting.

Service provider express rule set

For high load or hardware limited environments, the Service Provider Express rule set delivers effective spam detection at reduced hardware requirements.

This rule set provides the following features:

- Primarily based on signatures for known and active spam attacks
- Excellent message-per-second throughput and CPU stability
- Low false positive rate
- Best for minimizing hardware costs

Custom

In almost all cases, the full rule sets that Symantec provides meet the needs of our customers. In some cases, Symantec Security Response may make available a custom rule set available to a customer.

2 Click **Save & Continue**.

To set up notifications

The Notification Management panel is displayed.
On this panel, you can specify several types of notifications.

To specify that alert notifications be sent to up to 10 specific email addresses

1 To specify email addresses, check **Enable email notification**.

2 Enter the email addresses, separated by commas, into the **Email address** field.

3 Enter an email address from which you want the alerts to be sent into the **From** field.
The default address is for email alerts is `admin@hostname`.

4 Specify the address of the SMTP host that the appliance should use to send the notifications.

5 If necessary, specify the authentication credentials for the SMTP host.

Currently, Symantec Brightmail Traffic Shaper supports the CRAM-MD5 authentication scheme only.

6 To send a test message using the information you specified, click **Send test email**.

To specify a syslog server to which the appliance will send syslog event information

1. To enable syslog monitoring, check the **Enable syslog notification** checkbox.
2. Enter the IP address of the syslog host into the **Server** field.
3. From the drop-down list, select a syslog facility for Symantec Brightmail Traffic Shaper.
   You can choose from `local0` to `local6`, `user,` or `kern`. You must choose `kern` if you want to log connection shaping activity to a remote syslog server. If you have enabled outbound scanning for spam, choose `kern` to log the message that a sender IP address has been moved to bucket 6 and can no longer send email internally or externally.
   See "Filtering outbound mail for spam" on page 60.
4. Choose either **None**, **Log for all IP addresses**, or **Log for the following IP/ CIDR range only**.
   This option only applies to connection shaping action logging.

Warning: Logging connections from all IP addresses can severely impact performance.

If you chose either **Log for IP addresses** or **Log for the following IP/CIDR range only**, you can choose any or all of the following options:

- Log when Blacklisted path is rejected
- Log when path traffic is rejected for exceeding connection limit per bucket
- Log when traffic is dropped as an Earlytalker is detected
- Log when new traffic comes or bucket change is observed
- Log when path traffic is rejected for exceeding connection limit per IP
- Log when path traffic is rejected for exceeding message limit per connection

To enable Simple Network Management Protocol (SNMP)

1. To enable SNMP data collection, check the **Enable SNMP** checkbox.
   You will specify a community string and trap destination IP. The trap destination IP is the IP of the machine to which Symantec Brightmail Traffic Shaper will send the SNMP events trapped by Symantec Brightmail Traffic Shaper. The community string is the "password" that you have designated for all SNMP-enabled hosts to use to communicate with the

SNMP server. Symantec Brightmail Traffic Shaper will trap events related to whether or not the paths database is full.

2 Click on **Download 8160 specific MIB** files to download the MIB for your hardware platform.

This will launch the help for Symantec Brightmail Traffic Shaper. The MIB files are linked from the top of the help file.

3 Enter the community string into the **SNMP Community String** field.

4 Enter the IP address of the machine to which the appliance will send trapped SNMP events in the **SNMP Trap Destination IP** field.

5 Click **Save & Continue**.

To set up UPS monitoring

1 To enable UPS monitoring, check the box and enter the conditions under which the appliance will shut itself down.

The appliance supports monitoring of USB attached APC UPS devices and graceful shutdown upon loss of AC power when any one of the following configurable conditions are met:

- Battery Level: If during a power failure, the remaining battery percentage (as reported by the UPS) is below or equal to the specified value.
- Runtime minutes: If during a power failure, the remaining runtime in minutes (as calculated internally by the UPS) is below or equal the specified value.
- Timeout minutes: If during a power failure, the UPS has run on batteries for Timeout minutes. If you have a Smart UPS, you will most likely want to disable this timer by setting it to zero and use the other settings to control when a shutdown is initiated.

Note: Assume that the product gracefully shuts down based on the above settings. If the BIOS is configured to return to the last state when power is restored, the product will not restart when power returns. Ensure that you configure your BIOS settings accordingly.

2 Click **Save & Continue**.

To set up data synchronization

The Data Synchronization panel is displayed.

Symantec Brightmail Traffic Shaper can share information about email paths with other Symantec Brightmail Traffic Shaper appliances. This function is often useful for organizations in which multiple Symantec

Brightmail Traffic Shaper appliances are installed, either as High Availability clusters or separate appliances protecting separate networks.

For more information about data synchronization, refer to "Synchronizing data between appliances" on page 52.

Note: If you have selected data synchronization, but all of the devices in question are not yet configured, some status alerts may occur indicating that these systems are unreachable. You can safely ignore these alerts until the systems are properly configured.

---

1 If you need NAT support, check the **Enable NAT Support** box and enter a unique identifier in the text box.

The identifier can be any combination of letters, numbers, hyphens or periods up to 64 characters in length.

If you do not know what NAT is, chances are you do not need to enable NAT support. Most users do not need this option enabled.

Caution: If you have a Management NIC installed and want synchronization traffic to flow over the management network, you must:

- Enable NAT support
- Use the IP address of the remote host's Management NIC
- Provide unique host IDs for each system

2 Enter the IP address of each client.

In the box labeled **IP**, enter a single IP address, and click **Add Synchronization**.

If you have enabled NAT support, you must also enter each box's unique Host ID in the field provided before clicking **Add Synchronization**.

If you have configured data synchronization, the Key Management panel is displayed, otherwise, proceed to step 4.

3 Do one of the following:

If this is a primary device:

- In the **Generate key pair** box, click **Generate Keys**.
  A public/private key pair is generated.
- Download the public and private keys to the machine you are using to access the Control Center and make a note of the location. The keys will download as a single file named `pub_pri_key.tar`.

If this is a secondary device:

- Browse for the public and private keys you generated for the primary appliance and upload them to this appliance.

4 Click **Save & Continue**.

To activate settings

The Current Settings panel is displayed.

1 Review the values displayed here.

Caution: When you activate the configuration the first time, Symantec Brightmail Traffic Shaper will reboot. When the appliance comes back up, it will start bridging/routing for all protected servers defined. You MUST move the protected servers behind the appliance at this time. For subsequent changes to configurations, the appliance will require a reboot if you change the following settings: hostname, default gateway, advanced routes, configuration type (routed vs.bridged), and any of the settings on the Interfaces panel.

---

2 If the values are correct, click **Activate**.

If the values are not correct, you can click on an underlined section name to change values in that section.

Next you will be asked to reboot the appliance, or you can click **Cancel** if you do not want to make the configuration changes you specified.

Note: When Symantec Brightmail Traffic Shaper first starts up, it will be monitoring email traffic in Passthrough mode. It is recommended that you leave the appliance in this mode for approximately 24 hours, and then proceed to stage 1 of Traffic Control. If you remain in Passthrough mode, or in stages 2-4 for more than 5 days, the system status will change to **Warning**. If you remain in a stage other than stage 5 for more than 7 days, the system status will change to **Error**. For information about Passthrough and Traffic Control modes, refer to "Changing Traffic Control levels" on page 61.

Configuring multiple appliances

The most efficient way to configure multiple appliance deployments is to follow the Setup Wizard to configure the first appliance, save that configuration to the machine you are using to access the Control Center using the Export Settings option, then log into the Control Center on the other appliances and use the Import Settings option to import the same configuration. This will import all the settings you specified for the first appliance, including any public/private key pairs you need for data synchronization. You can then alter the configuration as needed for the subsequent appliances.

To configure multiple appliances

- On the first appliance, once it is fully configured:

1. Using a browser, log into the Control Center as the admin user.
2. Click **Settings**, then click **Export Settings** in the left hand menu.
3. Save the settings file to disk.

- On the second appliance:

4. Initialize the appliance as described in "Initializing Symantec Brightmail Traffic Shaper" on page 32.
5. Register the appliance as described in "Registering your appliance" on page 34.
6. Log into the Control Center.
7. Click **Settings**, then click **Import Settings** in the left hand menu.
8. Import the previously saved settings.
9. Click **Edit Settings** in the left hand menu.
10. Start the Setup Wizard.
    The settings you will have to change are:
    - DNS Setup - Hostname
    - Bridged vs Routed - if this is a high availability installation, set this system to the secondary appliance
    - Bridged/Routed Configuration Information - change the IP addresses
    - Data Synchronization – delete the current appliance IP address and add the IP address of the first Symantec Brightmail Traffic Shaper
11. Activate the configuration.

About configuration

When you complete the Setup Wizard described in "Setting up your appliance" on page 35 and activate your settings at the end, the previously saved settings are backed up, and your new settings are activated.

Exporting a configuration

You can export your current configuration settings to a local file and load them later.

To export your current configuration settings

1 From the Control Center, click **Settings**, then click **Export Settings** in the left menu.
The **Export Settings** page is displayed.

2 Click **Export settings**.
The File Download dialog is displayed.

3 Specify where you'd like to save the configuration settings file, and click **OK**.
The configuration settings file is saved for later use.

Importing an existing configuration

You can import and load configuration settings that you have previously exported using the instructions in "Exporting a configuration" on page 50. The configuration settings file you wish to import must be accessible from the machine you are using to access the Control Center.

To load configuration settings you saved manually

1 From the Control Center, click **Settings**, then click **Import Settings** in the left menu.
The Import Settings page is displayed.

2 Browse for the configuration settings file you wish to load and select it.

3 Click **Import Settings**.

Reverting settings

If you decide not to complete the Setup Wizard, you can revert to the current active settings, throwing away any change you made.

To revert to the current configuration settings

1 From the Control Center, click **Settings**, then click **Revert Settings** in the left menu.
The Revert Settings page is displayed.

2 Click **Revert Settings**.

Synchronizing data between appliances

Symantec Brightmail Traffic Shaper has the ability to share information on email paths with other Symantec Brightmail Traffic Shaper appliances. This function is often useful for organizations in which multiple Symantec Brightmail Traffic Shaper appliances are installed, either as High Availability clusters or separate appliances protecting separate networks.

By sharing data, the individual appliances avoid having to perform the redundant learning of identical data. This result means attackers who attempt to deliver spam to one ingress point on your network will have little to no success at an alternate ingress point, because the synchronized Symantec Brightmail Traffic Shaper on the other network is already aware of the threat.

In most cases, implementation of synchronization only requires the IP address of the Symantec Brightmail Traffic Shaper from which you wish to synchronize data. Key pairs will need to be generated on the master device on the “Key Management” page and then copied to the secondary device(s) via their individual Control Centers. All boxes attempting to synchronize data with each other must utilize the same key pair.

In some network environments administrators may choose to deploy devices in separate environments by utilizing Network Address Translation (NAT). In this scenario, it is possible that the publicly addressable IP address of the system is different from the private one. If this occurs, in order to facilitate proper communication between the Symantec Brightmail Traffic Shaper appliances, a unique host identification string should be specified. This is done via the Data Synchronization panel on the Settings page. Click the “Enable NAT Support” box and enter a unique identifier in the text box. The identifier can be any combination of letters, numbers, hyphens or periods up to 64 characters in length.

If you do not know what NAT is, chances are you do not need to enable NAT support. Most users do not need this option enabled.

Note: If data synchronization is selected, but all of the devices in question are not yet configured, some status alerts may occur indicating that these systems are unreachable. These alerts can be safely ignored until the systems are properly configured.

To set up data synchronization

1 From the Control Center, click on the **Settings** tab, and then click **Edit settings**, then **Synchronization**.

2 If you need NAT support, enable it now. (See the explanation of NAT above. Few networks will need this option.)

3 Enter the IP address of each client.

In the box marked **IP**, enter a single IP address, and click **Add synchronization**. If you have enabled NAT support, you must also enter each box's unique Host ID in the field provided before clicking **Add synchronization**.

4 If you have enabled NAT support, enter the unique Host ID for the box you are currently configuring in the "Local Host ID" box. If you have not enabled NAT support, skip this step.

5 When you are finished, click **Save & Continue**.

The Key Management panel is displayed.

6 A key pair will be automatically generated. You may use the pair generated or generate a new key pair by clicking **Generate Keys**.

7 Download the key pair by clicking **Download Keys**.

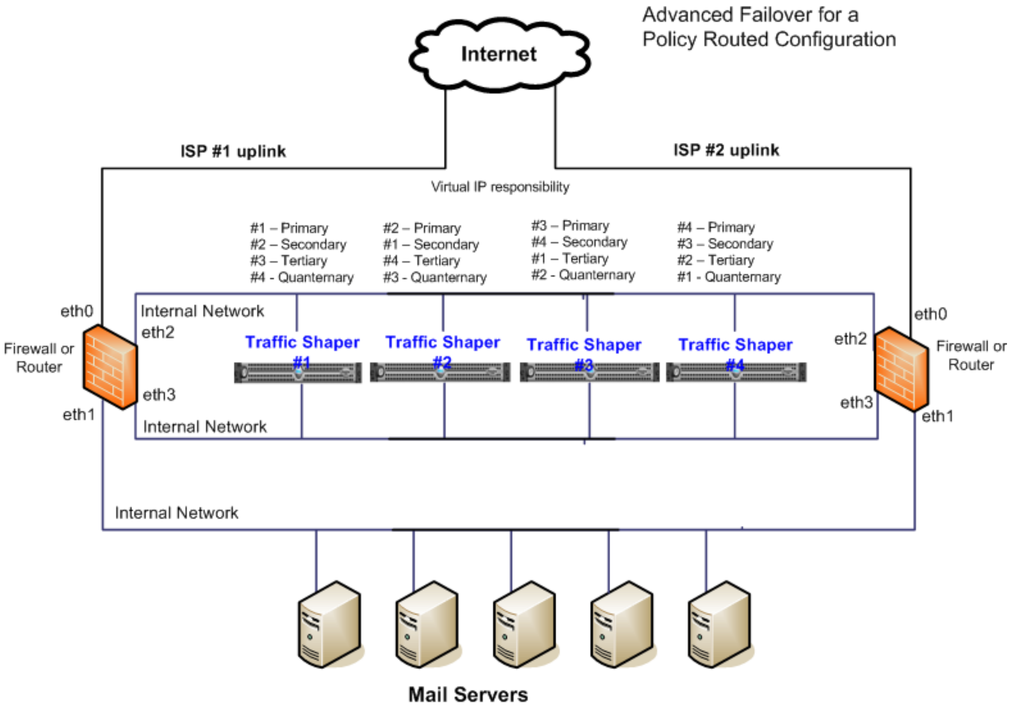
The keys will download as a single file named `pub_pri_key.tar`. Save this file, and upload it to the other appliances you plan to synchronize with when you configure them.

About advanced failover

Advanced failover allows an appliance to participate as a primary or backup device in a single cluster of up to four devices, or up to four different clusters.

It is intended to offer a high level of redundancy in dual-homed, policy routed configurations such as the one shown in Figure 3-1.

Figure 3-1 Advanced failover example



In this implementation, redundant connections from separate Internet Service Providers send email to the Firewall/Routers. Policy routes distribute email through the four Symantec Brightmail Traffic Shaper appliances, where the email streams pass through traffic control before they are sent back through the routers to the mail servers. For more details on this example implementation, refer to "Example advanced failover configuration" on page 57.

Required IP addresses

Each Symantec Brightmail Traffic Shaper in an advanced failover configuration requires four IP addresses:

- "Real"IP for Interface 1 – where the Control Center is available
- "Real" IP for Interface 2
- "Virtual" IP for Interface 1 – where incoming SMTP traffic gets forwarded by the router
- "Virtual" IP for Interface 2 – where return SMTP traffic gets forwarded by the router

For a full, four way failover setup, a total of 16 IP addresses are required for the Symantec Brightmail Traffic Shaper appliances, plus four for the firewall/router devices.

Virtual IP responsibility level

Each Symantec Brightmail Traffic Shaper is assigned a level of responsibility for each of the virtual IP addresses assigned to the cluster. The responsibility level defines the order in which an appliance will take over for a set of virtual IP addresses and respond to ARP requests for that address.

They are ranked in order of priority:

- Primary: assign the virtual IPs to this appliance if it is up
- Secondary: first level backup for a virtual IP
- Tertiary: second level backup for a virtual IP
- Quarternary: third level backup for a virtual IP

Virtual Router IDs

Each set of Virtual IP addresses must be assigned a Virtual Router ID. For each pair of virtual IP addresses set, the Virtual Router ID must be unique to the subnetwork the on which Symantec Brightmail Traffic Shaper appliances are located.

Configuring advanced failover

If you have multiple pairs of Symantec Brightmail Traffic Shaper appliances and want to configure them for advanced failover, you can edit each appliance’s configuration to do so.

To use this feature, all appliances must be operating in routed mode, where each interface of the appliance is on a different IP subnetwork. The policy routes must be defined so that email traffic entering the network through a particular Symantec Brightmail Traffic Shaper must return to its source through the same appliance.

Note: Importing a configuration file from Symantec Mail Security 8160 will fail and is unsupported.

To set up advanced failover

1. Edit the appliance configuration as described in "Configuring Symantec Brightmail Traffic Shaper" on page 36.
2. When you reach the **Bridged vs. Routed** panel, select the **Routed** radio button from the **Configuration Type** box and the **Advanced** radio button from the **High Availability** box.
3. Click **Save & Continue**.
4. Enter the information for a routed configuration as described in "To set up interfaces" on page 39.
5. Click **Save & Continue**.
   If you chose the **Advanced Routes** option on the **Configuration Setup** panel, the **Advanced Routes** panel is displayed.
6. Set up network routes as described in "To set up network routes and protected servers" on page 41, and click **Save & Continue**.
   The **Advanced Failover** panel is displayed.
   Each of the four columns represents one of up to four clusters.
7. Specify the appropriate internal and external virtual IPs and Virtual Router IDs for the appliance in the context of each cluster.
8. Choose the level or responsibility the appliance has in each of the clusters using the drop-down menus.
   The appliance can serve as the primary, secondary, tertiary, or quaternary failover machine.
9. Click **Save & Continue** and proceed through the Setup Wizard until you reach the **Activate Settings** panel, and activate your settings.

Example advanced failover configuration

This section describes the information needed for the example configuration in Figure 3-1.

Using the example, the following Virtual IP addresses will be assigned as the "primary" responsibility of the given appliance:

Table 3-1 Primary virtual IP addresses

Appliance unit #	External virtual IP	Internal virtual IP	Virtual Router ID
1	192.168.1.210	192.168.8.210	110
2	192.168.1.211	192.168.8.211	111
3	192.168.1.212	192.168.8.212	112
4	192.168.1.213	192.168.8.213	113

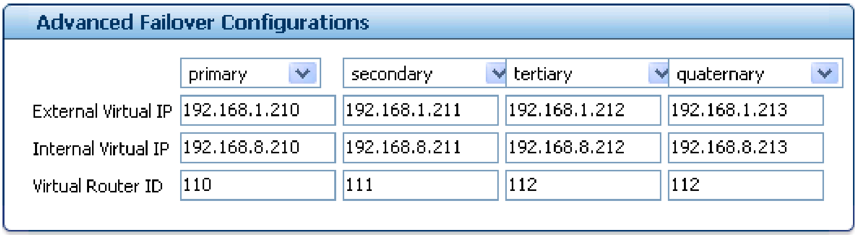
The backup responsibilities are as follows:

Table 3-2 Backup virtual IP addresses

Interface 1 virtual IP	Appliance #1	Appliance #2	Appliance #3	Appliance #4
192.168.1.210	Primary	Secondary	Tertiary	Quaternary
192.168.1.211	Secondary	Primary	Quaternary	Tertiary
192.168.1.212	Tertiary	Quaternary	Primary	Secondary
192.168.1.213	Quaternary	Tertiary	Secondary	Primary

The Control Center Advanced Failover Configurations pages for each appliance in this example look like this:

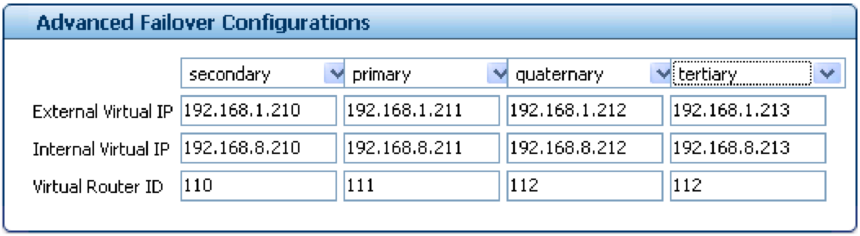
Figure 3-2 Symantec Brightmail Traffic Shaper #1



Advanced Failover Configurations

	primary	secondary	tertiary	quaternary
External Virtual IP	192.168.1.210	192.168.1.211	192.168.1.212	192.168.1.213
Internal Virtual IP	192.168.8.210	192.168.8.211	192.168.8.212	192.168.8.213
Virtual Router ID	110	111	112	112

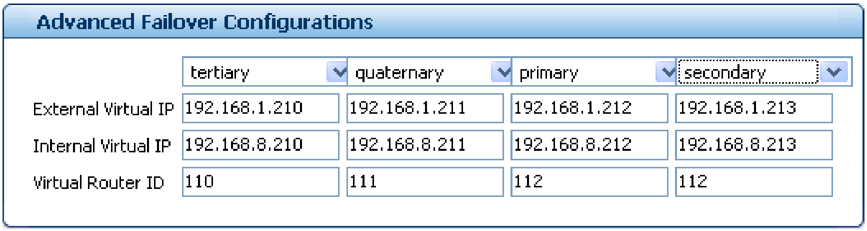
Figure 3-3 Symantec Brightmail Traffic Shaper #2



Advanced Failover Configurations

	secondary	primary	quaternary	tertiary
External Virtual IP	192.168.1.210	192.168.1.211	192.168.1.212	192.168.1.213
Internal Virtual IP	192.168.8.210	192.168.8.211	192.168.8.212	192.168.8.213
Virtual Router ID	110	111	112	112

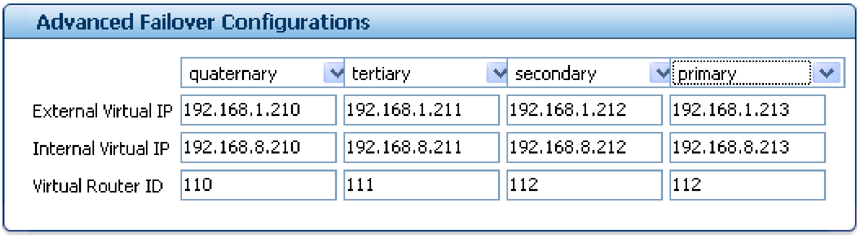
Figure 3-4 Symantec Brightmail Traffic Shaper #3



Advanced Failover Configurations

	tertiary	quaternary	primary	secondary
External Virtual IP	192.168.1.210	192.168.1.211	192.168.1.212	192.168.1.213
Internal Virtual IP	192.168.8.210	192.168.8.211	192.168.8.212	192.168.8.213
Virtual Router ID	110	111	112	112

Figure 3-5 Symantec Brightmail Traffic Shaper #4



Advanced Failover Configurations

	quaternary	tertiary	secondary	primary
External Virtual IP	192.168.1.210	192.168.1.211	192.168.1.212	192.168.1.213
Internal Virtual IP	192.168.8.210	192.168.8.211	192.168.8.212	192.168.8.213
Virtual Router ID	110	111	112	112

Working with Traffic Control

This chapter includes the following topics:

About Traffic Control

Traffic Control is how Symantec Brightmail Traffic Shaper prevents spam from entering the network by applying TCP traffic and connection shaping to a source network path. Symantec Brightmail Traffic Shaper applies traffic and connection shaping based on configuration policy that the administrator can select or manipulate.

Symantec Brightmail Traffic Shaper can be in one of three traffic control states:

- Inactive - Incoming email is being passed through the appliance, but is not being analyzed or traffic controlled; refer to "Stopping services (switching to Inactive mode)" on page 94.
- Passthrough - Incoming email is sampled and the spam rating for each path is updated, but no traffic control is applied.
  This is the default state for the appliance when first configured.   It is recommended that the appliance remain in this state for a minimum of 24 hours to get a representative sample of the incoming email traffic before switching to "active" mode.

- Active – Incoming email is sampled and the spam rating for each path is updated. Quality of service, including allowed bandwidth, concurrent connections, messages per connection and reconnect timeout (connection frequency), is enforced.

The real time status of traffic control is displayed in the Control Center at the top right side of the page.

There are some systems that you should consider whitelisting immediately:

- Other internal SMTP servers that send mail to your systems
- Systems on the External side of Symantec Brightmail Traffic Shaper that monitor your protected mail servers
  These systems typically connect to the SMTP server and then immediately quit the conversation. Since they never send a mail message, they fall into the “default” category which limits the number of concurrent connections and number of connections per second they are allowed. This could trigger false “down” alerts.

Filtering outbound mail for spam

Symantec Brightmail Traffic Shaper can filter outbound mailflow for spam. However, this feature only applies to router mode deployments, and the appliance must be configured to scan outbound mailflow only. Traffic Shaper does not support inbound mail processing and outbound mail processing on the same box.

See “Router Mode” on page 21.

See “Initializing Symantec Brightmail Traffic Shaper” on page 32.

As Symantec Brightmail Traffic Shaper analyzes outbound mail, it places the sender IP address into buckets. The buckets (numbered 1 - 9) correspond with the amount of spam email that the IP address sends. The higher the bucket number, the more spam email that the sender IP address is sending. When a sender IP address sends more than 75% spam, the sender IP address is placed into bucket 6. When Traffic Shaper places a sender IP address in bucket 6 a message is logged to the syslog, if configured, and locally to data/logs/messages. Sender IP addresses in bucket 6 or higher cannot send any email within or outside of the organization.

See “To specify a syslog server to which the appliance will send syslog event information” on page 46.

See “Viewing the Event Log” on page 74.

If the appliance has been set for inbound scanning and the Passthrough mode was enabled, when you enable the Outbound stage, the paths in buckets 6 through 9 can no longer send email. There will be no syslog messages to notify the administrator.

To remove a sender IP address from the blacklist, you must erase the path's history.

See "Modifying network path information" on page 86.

You must have System privileges or Master Administration privileges to change Traffic Control settings.

Filtering outbound mail for spam

1 From the Control Center, click **Administration**, then click **Traffic Control** in the left menu.

2 Under Stages, click **Outbound**.

Changing Traffic Control levels

You must have System or Master Administration privileges to change the Traffic Control level of Symantec Brightmail Traffic Shaper.

It is recommended that you start in Passthrough mode, spend about 24 hours gathering data in this mode, and then move up through the stages of Traffic Control at a rate of about 1 stage per 5-7 days until you reach stage 5. Most installations function optimally at stage 5 for the long term. You may also create a custom stage for your particular installation.

Note: If you remain in Passthrough mode, or in stages 2-4 for more than 5 days, the system status will change to **Warning**. If you remain in a stage other than stage 5 for more than 7 days, the system status will change to **Error**.

Changing Traffic Control to Passthrough mode

Setting Symantec Brightmail Traffic Shaper to Passthrough mode allows it to sample incoming traffic and "learn" about your site's traffic shaping needs.

Note: This is the default state for Symantec Brightmail Traffic Shaper when first configured.   It is recommended that the appliance remain in this state for a minimum of 24 hours to get a representative sample of the incoming email traffic before switching to "active" mode.

Outbound scanning does not support the use of the Passthrough mode. If the Passthrough mode has been enabled and then you enable the Outbound stage, the paths in buckets 6 through 9 can no longer send email.

See “Filtering outbound mail for spam” on page 60.

To set the appliance to Passthrough mode

1. From the Control Center, click **Administration**, then click **Traffic Control** in the left menu.
2. Select the **Passthrough** radio button.
3. In the confirmation dialog box, click O**K**.

Changing the level of active control

Traffic Control is normally applied in stages, to allow for analysis of the effect it has on the incoming email stream. When you initially activate Symantec Brightmail Traffic Shaper Traffic Control, it is at Stage 1. When you are satisfied that the appliance is working correctly, you can increase the Traffic Control level to Stages 2 through 5. An additional customized Stage 5 offers more aggressive Traffic Control for larger installations. Depending on how much traffic passes through your system, you should expect to run Symantec Brightmail Traffic Shaper at each stage for 5-7 days before moving on to the next stage.

To change the Traffic Control stage

1. From the Control Center, click **Administration**, then **Traffic Control**.
   The Traffic Control page is displayed.
2. Select the radio button for the Traffic Control stage you want to activate. Higher numbers indicate more control.
3. In the confirmation dialog box, click O**K**.

Tuning Traffic Control manually using a custom stage

You can tune aspects of Symantec Brightmail Traffic Shaper Traffic Control configuration manually by editing the configuration files.

Warning: Manually editing the traffic control files is normally unnecessary. Changes to traffic control must be made with extreme caution as undesirable results may occur if these parameters are not configured properly.

To edit a Traffic Control configuration file

1. From the Control Center, click **Administration**, then **Traffic Control**.
   The Traffic Control page is displayed.

2. Select the **Custom** radio button and click **Edit Custom**.
   If you have already customized one or more Traffic Control configuration files, you can select the one you want to edit from the drop-down menu.
   The Edit Traffic Control page is displayed.

3. Select the radio button for the Traffic Control configuration file you want to edit, and click **Edit**.
   You can use an existing Traffic Control configuration file as a template for a custom configuration file by either:
   - Downloading it and saving it with a new filename and then re-uploading it using the Upload Configuration File functionality, or
   - Selecting it for editing and then renaming it on the Edit page.

   The Edit Traffic Control page is displayed.
   The Classification column lists the breakdown of spam percentage ratings for which traffic control is configurable. There are control levels for default (or unknown) paths, and for paths that are 0-3% spam, 4-10% spam, 11-50% spam, etc.
   The rest of the columns define parameters that are configurable for each of the Classification ratings.
   The following are configurable values:

4. Overflow Bucket (denoted in the column beneath the asterisk (*)) – This radio button allows you to select which classification to apply to connections from new paths when Default is full. When Default has no more available connections to allocate, the Overflow Bucket indicates the classification level that will be examined first when looking for an available connection slot. If that level is also full, examination continues as described above.

- Threshold – The minimum number of messages that must be received from a path before it will be included in this classification level. If fewer messages have been received, the path will be included in the next most appropriate classification. For the best classification level, this means that connections will be shunted into the next worse level. For all other classification levels with a threshold value, a connection not meeting the specified threshold will be shunted up the levels until it satisfies a classification level's threshold value. All source network paths satisfy the threshold value for a level that has no threshold allocated.

- Connection Limit – The total number of simultaneous connections allowed for all paths at this classification. Connections that are evaluated to belong in one classification level will be shunted to the next lower level if the classification level has no more available connections. In this case, the connection will be treated to the same resource limits as any of the classification level's other connections.

  If you are scanning outbound mail, to ensure that a sender IP address cannot send email, set the conn_limit for the bucket to zero.

- Bandwidth/Connection – The total bandwidth in kilobits/second allowed for any given connection at this classification. You can specify bandwidth with this in mind, or you may find it more appropriate to think about the total message ingress into your network when setting this figure.

  Table 4-1 shows an estimate of the relationship between the kilobits/second value and the number of 10kb messages per hour. For example, to limit a certain message classification to approximately 40 messages per hour, set kbits/s to 1.

Table 4-1 Estimated kbit/second per messages/hour

kbit/s	msgs/hour
1000	40500
800	32400
700	28350
600	24300
500	20250
250	10125
100	4050
50	2025
10	405
8	324
7	283
6	243
5	202
4	162
3	121

Table 4-1 Estimated kbit/second per messages/hour

kbit/s	msgs/hour
2	81
1	40
0.9	36
0.8	32
0.7	28
0.6	24
0.5	20
0.4	16
0.3	12

- Connections/IP – The maximum number of simultaneous connections per path allowed. Subsequent connection attempts by a path after it reaches this limit will be rejected as long as all of the previous connections are still open.
- Msgs/Connection – The maximum number of messages per connection from a path allowed. When a source attempts to send more messages in a single connection, the connection is closed by Symantec Brightmail Traffic Shaper.
- Connection Timeout – The number of seconds that connection attempts from a given path will have to wait before they can reconnect after a path has met its Connections/IP value. The timeout is applied from the beginning of each connection. Connections attempted from a path before the timeout has expired will be rejected. Symantec recommends setting the connection timeout to 180 seconds or less.

5. To edit a value, select its current value and type in the new value.
6. When you have finished editing, click **Save**.
7. In the confirmation dialog box, click **Yes**.
   The Traffic Control page is displayed.
8. To activate the configuration you just edited, select its radio button.
   Your new configuration is activated.

Chapter 5

Working with graphs and reports

This chapter includes the following topics:

Viewing current path statistics

When you log into Symantec Brightmail Traffic Shaper, you see the Current Statistics page. You can also see this view when you click the Status tab.

This page gives a live, dynamically updated dashboard of clickable mini-graphs that show path quality, CPU utilization, message load, and bandwidth utilization. To see larger, more detailed views of each graph, click on the graph itself.

The Path Quality Statistics graph provides a live view of the breakdown of message quality. The green line denotes messages that have a 0% - 10% likelihood of being spam. The yellow line denotes messages that have a 11% - 75% likelihood of being spam. The red line denotes messages that have a 76% - 100% likelihood of being spam. The gray line denotes messages from paths which have not been classified yet.

Information is also provided about the number of connections, how much bandwidth (in bits) is being used, the message load in messages per second, and the path quality, described as ‘clean’, or ‘mixed’, and the number of spam messages per second.

Caution: If at some point you set the time of the appliance back to an earlier time, you may see an error describing a problem with the statistics database. This error occurs because the timestamp on the data currently being collected is interpreted as being older than a previous entry. The error message provides a link you can click to change the timestamps of the “invalid” entries to the current time which will allow the appliance to resume entering data into the database. This may result in these points showing up as a spike in the data at the beginning of the graph.

Viewing available graphs

The **Status** section provides both current and historical information about the operations of your Symantec Brightmail Traffic Shaper installation in graphical form. This section describes the following available line graphs:

- Connection load graph
- Bandwidth utilization graph
- Message load graph
- Filtered path quality graph
- CPU utilization graph

Along with the graphical data, a table of the data points used to build the graph is also displayed beneath each graphical representation.

Note: When statistics include a value for the number of messages transmitted, any SMTP transaction is counted as a "message," even if the mail server terminated the transaction prior to the message being accepted. For example, an SMTP transaction that is terminated by the mail server after the RCPT TO command because the envelope recipient is unknown will be counted by Symantec Brightmail Traffic Shaper even though the transaction never reached the DATA stage. This distinction may cause the statistics on Symantec Brightmail Traffic Shaper to differ from those displayed by mail servers protected by Symantec Brightmail Traffic Shaper.

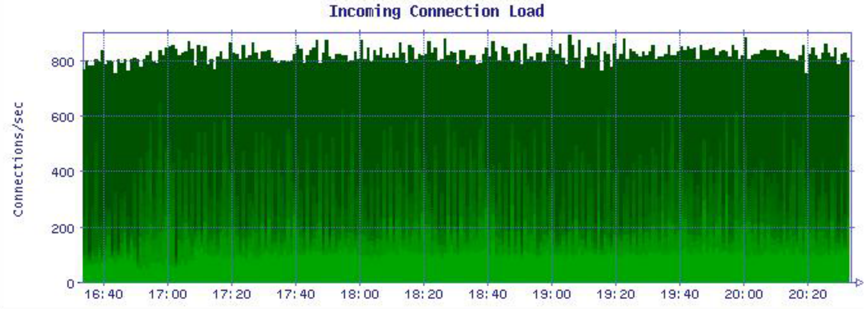
To view current statistics and historical data in graph form

◆ From the Control Center, click **Status**, then click the name of the graph you would like to see in the menu on the left.

Connection load graph

The Connection Load graph displays the number of SMTP connections made per second to your protected servers.

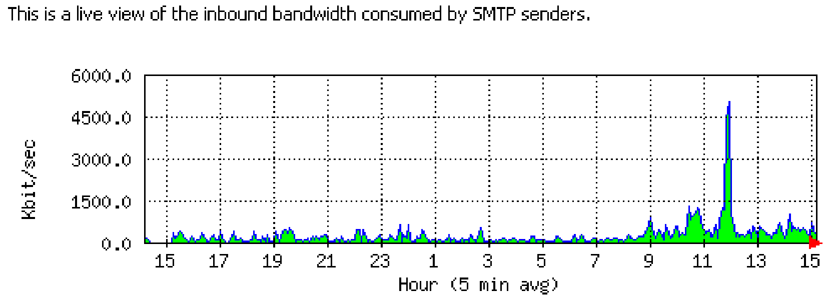
Figure 5-1 Sample connection load graph



Bandwidth utilization graph

The Bandwidth Utilization graph shown in Figure 5-2 displays SMTP traffic passing across Symantec Brightmail Traffic Shaper from the external interface toward the protected network, expressed in bits per second. This graph does not track non-SMTP traffic that may also be traversing the appliance.

Figure 5-2 Example bandwidth utilization graph

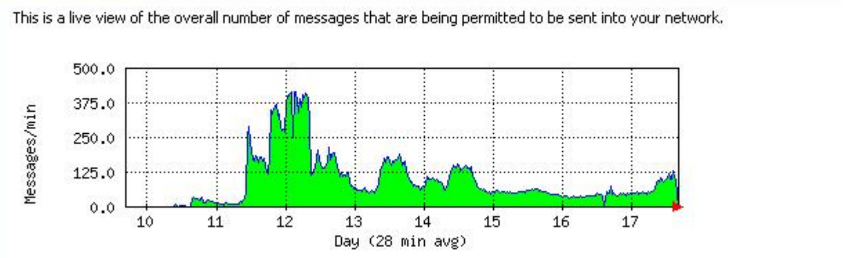


This is a live view of the inbound bandwidth consumed by SMTP senders.

Message load graph

The Message Load graph shown in Figure 5-3, shows the overall rate of messages per second that have been allowed into your network over time.

Figure 5-3 Example message load graph



This is a live view of the overall number of messages that are being permitted to be sent into your network.

Filtered path quality graph

The path quality statistics graph shown in Figure 5-4 shows Symantec Brightmail Traffic Shaper's analysis of the quality of messages that have been sent from various paths into your network each second. The graph has four color-coded lines to illustrate different classes of messages:

Green Messages with a 0 to 10% likelihood of being spam (clean).

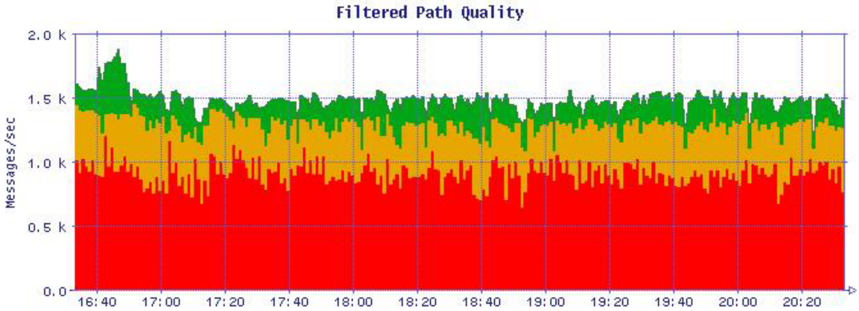
Yellow Messages with a 11 to 75% likelihood of being spam (mixed).

Red Messages with a 76 to 100% likelihood of being spam (spam).

Gray Messages that have not yet been classified.

The graph shows both the historical 24-hour data as well the current clean, mixed, and spam messages/second.

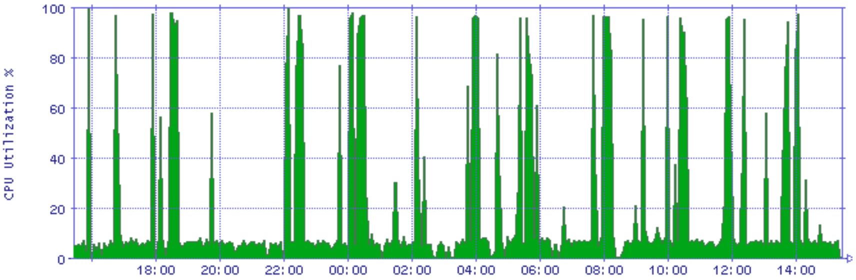
Figure 5-4 Path quality statistics graph



CPU utilization graph

This graph shows the percentage of CPU in use on Symantec Brightmail Traffic Shaper over time.

Processor load on the Appliance.



Modifying graph display and saving graph data

Each of the graphs can be modified to suit the time range that you would prefer for your reporting purposes. Additionally, you can export the data points used to construct the graphs in comma separated values (CSV) format for use in your own customized reporting or graphing applications.

Changing the graph time frame

You can change the time frame (and corresponding graph scale) of the data points that comprise the graph. You can choose to view a graph versus any one of the following graph time frames:

- Partial Day
- Day
- Week
- Month
- Year
- 10 years

To change the time frame of a graph

- On the graph page, in the timeframe drop-down box, select the new time frame.
  The graph and corresponding data table update automatically.

Exporting the graph data

You may also export the data table used to create the graphs in the Statistics page, in comma separated variable (CSV) format. This data may be imported into spreadsheet, database, or reporting programs for customized graphing and/or reporting.

To import the CSV file into another program, consult that program's documentation or help files.

To export graph data

1. Below the graph, click **Download this graph’s data**.
2. In the File Download dialog box, click **Save**.
3. In the Save As dialog box, type the location where the .csv file should be saved, and then click **Save**.

4 In the Download Complete dialog box, click **Close**.

Viewing current network statistics

The Network Statistics page contains the following three fields of information regarding the router and its role in your network:

- External network
- Protected network
- ARP table

To view network statistics

- From the Control Center, click **Status**, then click **Network Statistics** in the menu on the left.

  The Network Statistics page is displayed.

External network

The External network field contains information about the interface from the appliance to the external internet. The first part of the table shows packet volumes and error information for packets received and transmitted. This information may be useful in investigating network connectivity issues.

The configuration information for the interface is displayed in the second table.

Protected network

The Protected network field describes the interface from the appliance to the protected network (where your protected SMTP server is located). The first part of the table shows packet volumes and error information for packets received and transmitted. This information may be useful in investigating network connectivity issues.

The configuration information for the interface is displayed in the second table.

Arp Table

This table shows the contents of the ARP cache on the appliance and the interface the entry is located on.

Viewing System Status

The System Status page displays summary and detail status of the appliance, including System Uptime, Load Average, Rule updates, Software update availability, BRS updates, Path database backup and Failover status. The System Status page also provides information about hardware status: UPS, power supply redundancy, fans, RAID status, internal temperature, and CPU temperature.

Note: If you remain in Passthrough mode, or in stages 2-4 for more than 5 days, the system status will change to **Warning**. If you remain in a stage other than stage 5 for more than 7 days, the system status will change to **Error**. For information about Passthrough and Traffic Control modes, refer to "Changing Traffic Control levels" on page 61.

Note: You can also reach System Status page from anywhere within the Control Center by clicking on the **Status** link on the right hand side of the tab bar. The tab bar displays the current overall status of the appliance. If any of the items on the System Status page are not functioning correctly, the status displayed for the overall appliance will be WARNING.

To view System Status

- From the Control Center, click **Status**, then click **System Status** in the menu on the left.
  The System Status page is displayed.

Viewing the Event Log

The Event Log displays all administrator actions and alerts issued.

To view the Event Log

- From the Control Center, click **Status**, then click **Event Log** in the menu on the left.
  The Event Log page is displayed.

Viewing overall path statistics

The Path Statistics page contains a table that shows a detailed breakdown of the classifications of all network paths that have sent email into your network. As email traffic enters your network, Symantec Brightmail Traffic Shaper analyzes the traffic originating from that network path and assigns a classification to that path based on the appliance's determination of the likelihood that it is sending spam into your network. The lower the percentage, the less likely spam is being sent on the specific path.

To view classifications of network paths

- From the Control Center, click **Reports**.
  The Path Statistics page is displayed.

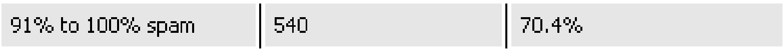
The Path Statistics page provides the following information about classifications of network paths.

Table 5-1 Path Statistics page information

Column	Description
Path Classification	Shows the categorization of the approximate spam received from various paths.
Number of Paths	Shows the total number of paths known to be producing the levels of Spam seen in column 'Path Classification'.
Percentage of Total	Shows the percentage relative to the total amount of email traffic going through Symantec Brightmail Traffic Shaper.

Figure 5-5 shows an example of detail from the Path Statistics page.

Figure 5-5 Path Statistics page detail



91% to 100% spam	540	70.4%

This detail shows that 90% - 100% of the mail analyzed from these 540 paths has been identified as spam, and comprises 70.4% of all paths stored in the database.

The Path Statistics page also displays the total number of network paths that are known to be sending email traffic into your network as well as a time stamp showing the time this information was last updated.

Viewing email traffic estimates

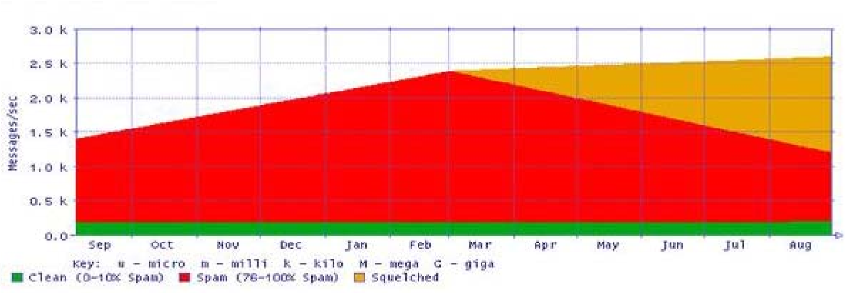
The email traffic graph shows emails that have been processed, and their projected amounts in the future, based on data collected while the appliance is in passthrough mode.

Note: At least one day's worth of e-mail with the appliance in passthrough mode is required to generate this graph.

Once Symantec Brightmail Traffic Shaper has been placed in Active mode, this graph should no longer be referenced.

To view email load estimates

◆ From the Control Center, click **Reports**, then click **Email Estimates** in the menu on the left.
The Email Estimates page is displayed.



Viewing and creating reports

Using the Control Center, you can view and download the data from a number of preconfigured reports or create custom reports and save them for reuse later.

The following preconfigured reports are available:

- Path Quality (RCPTs)
  A RCPT is when an e-mail is sent to a unique recipient. This graph shows how many RCPTs were received per second, and breaks them down based on the quality of the path.
- Path Quality (Complete Transactions)
  A complete transaction is when a complete email is sent successfully. This graph breaks down the number of complete transactions per second based on the quality of the graph. The difference between a complete transaction and a RCPT is that the sending machine may break off the connection

before they finish sending the message. This graph only shows messages that were successfully sent.

- Transaction Activity
  This graph plots the following:
  - The number of SMTP transactions per second across all paths. SMTP Transactions can each include one or more RCPTs.
  - The number of RCPTs seen per second across all paths.
  - The number of messages that were properly ended.

  This graph can be used to determine if there are an abnormal number of messages that were not ended properly, OR if (on average) there is more than one recipient per message.

To display a preconfigured report

1. From the Control Center, click **Reports**, then click **View Report** in the menu on the left.
   The View Reports page is displayed.
2. Select the report you wish to view from the **Report** drop-down list, select the timeframe for which you wish to generate the report from the **Timeframe** drop-down list, and click **Generate Report**.
3. The report is generated.

To create a custom report

1. From the Control Center, click **Reports**, then click **Custom Reports** in the menu on the left.
   The Custom Reports page is displayed.
2. From the **Data Source** column, select a source of data to use from the drop-down list.
   For a description of each data source, refer to “Data sources for custom reports” on page 78.
3. From the **Classification** column, select a classification of data to graph from the first drop-down list.
4. From the **Color** column, specify the color line you want this data displayed in.
5. From the **Range** drop-down list, specify the timeframe for your report.
   If you select Custom, specify the start and end dates by clicking on the start and end dates that are displayed and choosing a date from the pop-up calendar.
6. Repeat steps 1-4 as needed for additional data sources and classifications.

7. If you need more than four sources, click **Add Row**.
8. When you have specified all the sources of data for the report, click **Generate Report**.
   The report is generated.
9. To add this report to your list of favorite reports, click **Add to Favorites** and enter a name for the report into the text box.

To display a favorite report

1. From the Control Center, click **Reports**, then click **Favorite Reports** in the menu on the left.
   The Favorite Reports page is displayed.
2. Select the report you wish to view from the drop-down list, and click **Run Report**.
3. The report is generated.
4. To edit the parameters of the report before generating, click **Edit** and make changes as described in "To create a custom report" on page 77.

To export report data

1. Below the report, click **Download this graph's data**.
2. n the File Download dialog box, click **Save**.
3. In the Save As dialog box, type the location where the .csv file should be saved, and then click **Save**.
4. In the Download Complete dialog box, click **Close**.
   To import the CSV file into another program, consult that program's documentation or help files.

Data sources for custom reports

The following is a list of the data sources available for use in custom reporting:

- Connection Attempts
  The number of connections to protected servers that were attempted, regardless of whether or not they resulted in an established connection.
- Connections Made
  The number of SMTP connections to protected servers that were actually established.

- Messages Seen
  The number of the SMTP transactions that were observed by Symantec Brightmail Traffic Shaper. This is not the same as the number of messages delivered to end users, as the protected server may bifurcate messages after Symantec Brightmail Traffic Shaper is no longer involved in the transaction. Additionally, SMTP transactions with multiple recipients are only counted once for this metric.
- Ends of Mails
  The number of SMTP transactions that were observed actually attempting to send mail. Examples of transaction ending events are the MAIL command after a previous transaction, an RSET command, a QUIT command or a connection tear down following an SMTP transaction. This does not include the number of RFC 2821 MAILEND sequences seen; this metric is described in the Message Endings data source.
- Recipients Seen
  The number of recipients seen during SMTP transactions. This metric is closer to the actual number of email messages received by end users but does not take into account refusal of recipients by the protected servers.
- Message Endings
  The number of SMTP transactions that were terminated specifically with an RFC 2821 MAILEND sequence (such as `<CR><LF>.<CR><LF>`).
- CPU Utilization
  The average load on the CPU at timed intervals on a range from 0 to 100 (0 meaning idle, 100 meaning the maximum load).
- Bandwidth
  The amount of bandwidth Symantec Brightmail Traffic Shaper uses to forward SMTP traffic.
- Blacklist Rejected
  The number of connections that were refused because their sources were blacklisted by an Administrator.

Chapter 6

Working with network path information

This chapter includes the following topics:

About network path information

Symantec Brightmail Traffic Shaper works by analyzing your network's mail flow and identifying the behavior of various network paths over time. All of this happens transparently, without the need for administrative intervention. You may want to make changes in response to current conditions.

Users have the following network path permissions:

Master administrator	Has full access to path administration.
Data administrator	Has access to all reports including the custom reports and has full access to path administration functions. The data administrator cannot view the Changelog and does not have access to settings and system control functions.
Path administrator	Able to view and modify path data. The path administrator has access to the standard reports, but cannot create custom reports. The path administrator cannot view the Changelog and does not have access to settings and system control functions. The path administrator's access to path administration is restricted. The path administrator does not have access to the Outbound Paths page, Backup / Restore Path data pages, Bulk Path Upload page and the DB Maintenance page. The path administrator can search for paths and edit them, and can add paths to Diagnosis per IP and view / download the logged messages.

Searching network path information

The Search function gives you easy access to network path information.

To search historical path data and its associated spam categorization, select the option for the paths that you want to search. You can limit your search by the type of path or the bucket into which Symantec Brightmail Traffic Shaper placed the path.

Table 6-1 shows the available limits.

Table 6-1 Network path search limiters

Limit	Description
All Paths	Include all paths in the specified IP, range, or domain. When you use this option with a CIDR/domain, all of the paths from that CIDR/domain appear, including the ones that are not in the database.
Available Paths Only	Include all available paths in the specified IP, range, or domain. When you use this option with a CIDR/domain, only the paths from that CIDR/domain that are present in the database appear.
All Administratively Altered Paths	Include all paths in the specified IP, range, or domain that were altered by an administrator.
Administratively Whitelisted Paths	Include all paths in the specified IP, range, or domain that were whitelisted by an administrator.
Administratively Blacklisted Paths	Include all paths in the specified IP, range, or domain that were blacklisted by an administrator.
Locked Paths	Include all locked paths in the specified IP, range, or domain.
Search Paths in Bucket	Include the paths specified by the selections above that are in the specified bucket.

To find more specific results, you can also search by the domain name, Classless Internet Domain Routing (CIDR) block or IP address of the network path.

Table 6-2 defines the search parameters.

Table 6-2 Network path search parameters

Search parameter	Format	Search results
IP Address	192.168.1.100	Paths originating at the host with IP address 192.168.1.100
Domain Name	fflanda.com	Paths originating from IP addresses that resolve to the MX record for domain name fflanda.com

Table 6-2 Network path search parameters

Search parameter	Format	Search results
CIDR Block	192.168.1.0/24	Paths originating from hosts in the subnet denoted by the class C address 192.168.0.0 (for example 192.168.1 ... 192.168.1.0.255)

Note: If you enter a domain name into the search field, only the IP addresses listed in the MX records are returned in the search results.

The search parameters in Table 6-2 combine with the limits in Table 6-1. For example, if you select one of the option button and click Submit, a report of all Admin Altered or Whitelisted or Blacklisted or Locked paths appear. If you select a bucket and click Submit, all of the paths in the database from that bucket appear. Also it is possible to search for all Admin Altered or Locked paths in a specific bucket.

The search results that appear show the first 1000 paths that meet the search criteria. If there are more paths that meet the search criteria, the complete result set can be downloaded from a link that is located above the search results.

To search network path information

1. From the Control Center, click **Paths**.
2. The Search/Modify Paths page is displayed.
3. Enter one of the following:
   - IP Address
   - Domain Name
   - CIDR
4. Click one of the following:
   - All Paths
   - Available Paths Only
   - All Administratively Altered Paths
   - Administratively Whitelisted Paths
   - Administratively Blacklisted Paths
   - Locked Paths
5. Optionally, click **Search paths in bucket** and choose a bucket number.
6. Click **Search**.

Note: You can also use the Path Search field on every page in the Control Center.

For each network path returned by the search, the approximate spam rate and path confidence are displayed. The spam rate is expressed as an approximate percentage of traffic from that path which is spam, and is color coded to reflect whether it is considered to be valid mail (green), spam (red), and mixed (yellow). The spam rate value also includes the number of the bucket that the network path has been assigned to. The path confidence indicates how confident Symantec Brightmail Traffic Shaper is in its analysis of that path.

- WL: Whitelisted
- BL: Blacklisted
- AA: Administratively Altered
- RM: from a Remote Machine in the cluster
- BRS: listed in the Brightmail Reputation Service
- BEIK: from a client customized using the Brightmail Engine Integration Kit
- LOCK: from a path for which you have specified a spam rating and locked (refer to “Modifying network path information” on page 86)

In some cases, the spam rate and path confidence are not displayed, but a single value is shown to express the status of that path. These special values are:

Unknown
No path data is available because insufficient traffic has been sent from that path to make a valid determination or the path information has been administratively deleted.

Whitelisted
The path has been administratively configured such that this path is being treated as a non-spam sending path.

Blacklisted
The path has been administratively defined such that it is considered to be a spam sending path.

If you use the Search Box to navigate to a path, you can make your changes directly from the Search Results page, if a single result is returned. If multiple results are returned, you can perform bulk modifications on all results returned, or you can change path information using the Path Administration page.

See “Making bulk changes to network paths” on page 88.

See “Modifying network path information” on page 86.

Modifying network path information

You can view, add or edit information about paths that you consider to be spam.

A key function of Symantec Brightmail Traffic Shaper operation is the analysis, over time, of email traffic from various network paths. This analysis is done and the results acted upon automatically, without any administrator intervention. However, certain situations may arise where you want to override settings and manually configure information about specific network paths.

You can change path information in one of the following ways:

Search Results page	Make changes to a network path based upon a hostname, domain name, IP Address, CIDR block, or various path characteristics.
`repupdate` command	You can use the repupdate command to remotely pipe an update file to the Symantec Brightmail Traffic Shaper that includes your path changes. See “repupdate” on page 115.

To modify a network path

1. In the Control Center, click **Paths**.
2. Search for the path you want to alter using the Search/Modify Paths page using the information in “Searching network path information” on page 82 and click on it.
   The Editing page is displayed.
3. If you want to add this path to the Whitelist or Blacklist, click the appropriate button.
   The path is immediately added to the specified list.
   - When a network path is administratively set to Blacklisted, Symantec Brightmail Traffic Shaper refuses all connections from that path.
   - When a network path is administratively set to Whitelisted, Symantec Brightmail Traffic Shaper gives maximum quality of service to connections from that path.
4. If you want to erase the recorded history for this path, click **Erase Path**.
   The history for this path is immediately erased. When you erase the recorded history of a path, the appliance's prior analysis of that path is discarded. It will start again as traffic from that path is analyzed in the future.
5. If you intend to lock a path, click the drop-down menu above Network Path Lock Option and select the assumed spam percentage rate.

6 To lock the path, under Network Path Lock Option, select one of the following options:

None	The path is not locked and can move to other buckets. This is the default setting.
Indefinite	The path is locked indefinitely and cannot move to other buckets. If you are migrating to Symantec Brightmail Traffic Shaper, any paths that you had locked are Indefinite.
Timed	The path is locked for the number of days that you specify. When the time period expires, the path is automatically unlocked. However, you can manually unlock the path prior to the expiration date by changing the setting to None. Type the number of days that you want the path locked. The default setting is 7 days. You can type a number between 1 - 999.

7 If this path is already in the Whitelist or Blacklist, locking it will have no effect.

8 Click **Update**.

Changing a path's assumed spam rate

You can change a path’s assumed spam rate manually from 0% to 100% spam to adjust how you want Symantec Brightmail Traffic Shaper to treat that specific path. This produces results as though the appliance were making its own conclusions about that path based on analysis over time, but with immediate results.

You may want to use this option to pre-configure Symantec Brightmail Traffic Shaper with information about paths it has not yet seen, or you may choose to override the appliance's analysis based on information you may have about a network path.

To change a path’s assumed spam rate

1 In the Control Center, click **Paths**.

2 Search for the path you want to alter using the Search/Modify Paths page using the information in “Searching network path information” on page 82 and click on it.
The Editing page is displayed.

3 Select the new spam rate from the drop down list.

4 If you want to lock this path, click the **Lock** checkbox.
Locking the path prevents other processes such as the Symantec Brightmail Traffic Shaper analysis module from updating the value for the path.

5 Click **Update**.

Making bulk changes to network paths

There may be times when you want to make changes to a number of network paths simultaneously. You can do this from any Search Results page where multiple results have been returned (for example, when your search criteria was a domain name or CIDR block).

You can use the following commands to make bulk changes to all network paths listed on the page:

Whitelist All	Mark all paths listed in the results table as 'whitelisted'.
Blacklist All	Mark all paths listed in the results table as 'blacklisted'.
Erase All	Erase analysis data for all paths listed in the results table.

Note: These options only appear if the number of paths in the search result is less than or equal to 256.

To make bulk changes to network paths

1 In the Control Center, click **Paths**.

2 In the Search text box, type one of the following:

- IP Address
- Domain Name
- CIDR

3 Click **Search**.
Review the results of the search to make sure you want to apply bulk changes.

4 In the right pane, click one of the following options:

- Whitelist All
- Blacklist All
- Erase All

Uploading whitelisted or blacklisted paths in bulk

You may have lists of network paths that you want Symantec Brightmail Traffic Shaper to automatically allow or disallow traffic from without doing any processing. You can upload whitelisted and blacklisted sender lists if you are logged in as a Data or Master Administrator.

The files you upload must be plain text and can contain individual IP addresses or CIDR blocks, one IP or CIDR block per line. The maximum size recommended netblock to upload at one time is a /16.

To upload allowed or blocked sender lists

1. In the Control Center, click Paths, then click on **Bulk Path Upload**.
   The Bulk Path Upload page is displayed.
2. From the appropriate section, browse for the file you wish to upload.
3. Click the **Upload** button for the type of list you're uploading.
   The file is uploaded to the appliance.

Maintaining the paths database

At 1:30am every day, a script cleans the paths database. The pruning algorithm works in two passes. There is a list of 365 counters that correspond to the last 365 days. The first pass runs through all entries in the asdb. For each entry increment, the counter that corresponds to the number of days old for this entry. The 365th counter counts entries that are 365 days or more. The loop also counts the total number of entries. When it finishes, it starts at the counter corresponding to the oldest entries. It accumulates the counters, starting at the oldest, until it finds the exact day where newer entries account for just less than 85% of the maximum size of the database. That is the day to which the database is pruned.

If the database is less than 85% full, then no BEIK entries are pruned. BRS entries more than one day old are always pruned. This process continues since they are updated daily.

Deleting administratively altered paths

You may from time to time wish to delete all of the altered records in the paths database. You may have received an alert notifying you that the database is at capacity, or you may wish to simply reset the number of administratively altered records to 0.

See “prune_asdb” on page 114.

To delete all administratively altered paths

1 In the Control Center, click **Paths**, then click on **Database Maintenance**.
The Database Maintenance page is displayed.
It is strongly recommended that you back up your database before deleting all administratively altered records. Use the Backup utility to do so, described in "Backing up path data" on page 90.

2 When you have backed up your data, click **Delete All Administratively Altered records**.

3 The records are deleted.

Backing up path data

You can back up all path data records to disk.

To back up the database

1 From the Control Center, click **Paths**, then click **Backup Path Data** in the menu on the left.
The Backup Path Data page is displayed.

2 Click **Backup Now**.
The Save dialog for your system is displayed. If you have no administratively altered path data to back up, you will see a message indicating this.

3 Choose where you'd like to save the backup file and save the file.

Restoring path data

You can restore the database of path information from a file to which you backed up earlier. To do this, you must be able to browse to the backup file from the machine you are using to access the Control Center.

To restore the database

1 From the Control Center, click **Paths**, then click **Restore Path Data** in the menu on the left.
The Restore page is displayed.

2 Browse for the backup file you made and select it.

3 Click **Restore**.

Note: If a path already exists, it will be overwritten. If a path in the file does not exist, it is added to the database.

Working with watched path data

This feature lets you specify up to 256 IP addresses, or paths, for which the appliance will monitor detailed information. Each message analyzed for that IP will be classified as spam or clean, based on the analysis of Symantec Brightmail Traffic Shaper.

For each IP you specify, you can do the following:

- Download all messages sent from this IP to disk
- View messages captured from this IP
- Delete messages sent from this IP

To specify paths to watch and view their data

1. From the Control Center, click **Paths**, then click **Diagnosis Per IP** in the menu on the left.

   The Diagnosis per IP page is displayed.

2. Enter a CIDR block or IP address and click **Add**.

   The block is added to the watched list. If you added an IP address, it will be converted into CIDR notation (/32).

   You can also upload a text file containing IPs or CIDR blocks that you want to watch, one IP or CIDR block per line. The total number of IPs that the list represents must not exceed 256.

3. To view the emails for an IP in the list that have been classified as clean or spam, click the **Clean Messages** or **Spam Messages** link for that IP.

4. To delete the messages for an IP in the list, click the **Delete messages from <IP>** link.

5. To download a zip file containing all the email messages for all watched paths, click **Download**.

Working with outbound path data

You can clear path history for paths you have specified as outbound. You can specify these paths during appliance setup, or at a later time.

To specify outbound paths

1. From the Control Center, click **Paths**, then click **Outbound Paths** in the menu on the left.

   The Outbound Paths page is displayed.

2. Click Manage Outbound Paths.

   The Outbound paths page is displayed.

3. Enter outbound paths for which you want Symantec Brightmail Traffic Shaper to control traffic.

   For installations that are shaping outgoing SMTP connections from internal systems, where the addresses are allocated through DHCP, the appliance is capable of periodically purging the path history. This allows the appliance to compensate when an IP address previously held by a spammer, which was severely traffic controlled, is reassigned to an unrelated system. Most likely, you will want to set the refresh rate so that it matches the DHCP lease time.

   If you have a large list of outbound paths to enter, you can upload a plain text file, with one IP address per line. For example:

   ```
   192.168.3.3
   192.168.3.4
   ```

4. To clear path history for outbound paths, click **Clear Now**.

Chapter 7

Administering Symantec Brightmail Traffic Shaper

This chapter includes the following topics:

Starting, stopping, or powering down

You can temporarily disable the antispam services of Symantec Brightmail Traffic Shaper, or shut it down to prepare for a move or for physical maintenance.

When Symantec Brightmail Traffic Shaper is first installed, it comes up in Passthrough mode, where no traffic control is applied. In Passthrough mode, the appliance examines mail from source Paths (IP addresses), rating the mail as to the probability it is spam, and recording the results for each Path in the internal database.

You can switch from Passthrough mode to Inactive mode for diagnostic purposes.

Stopping services (switching to Inactive mode)

You must be logged on as a Master or System Administrator to deactivate the antispam services of Symantec Brightmail Traffic Shaper.

Once you have stopped services, the status indicator in the upper right of the page displays the word **Inactive** in red. This status remains on all pages, for all user accounts, until Symantec Brightmail Traffic Shaper is started again.

Note: While services are Inactive, you cannot alter paths or perform any action other than manipulate the configuration. Graphs will no longer be updated and the paths database is inaccessible.

To stop Symantec Brightmail Traffic Shaper services

1. From the Control Center, click **Administration**, then click **System Control** in the left pane.
2. In the right pane, under Adjust Appliance State, click **Turn Off**.
3. On the Confirmation page, click **Yes**.
   If you do not want to deactivate filtering services, do one of the following:
   - Click **Cancel.**
   - On your browser, click **Back**.

You also can completely power down the appliance. See “Powering down and rebooting the appliance” on page 95.

Starting services (switching to Active mode)

You can reactivate Symantec Brightmail Traffic Shaper antispam services after they have been manually stopped. Once the appliance is reactivated it will resume analyzing email sources and reducing spam.

To start Symantec Brightmail Traffic Shaper services

1. From the Control Center, click **Administration**, then click **System Control** in the left pane.
2. In the right pane, under Adjust Appliance State, click **Switch to Active**.

Powering down and rebooting the appliance

You can power down Symantec Brightmail Traffic Shaper in preparation for moving, network maintenance, or other situations that require that it be powered off. You can also reboot the appliance.

To power down or reboot Symantec Brightmail Traffic Shaper

1. From the Control Center, click **Administration**, then click **System Control** in the left pane.
2. In the right pane, under Power Appliance Down, click **Power Down**.
3. If you want to reboot the appliance, click **Reboot**.

Changing the database size limit

Symantec Brightmail Traffic Shaper is shipped with a default maximum database size of 20 million IP addresses. You can change the maximum size, to 10 million, 20 million, or 50 million IP addresses.

Note: If your current database is larger than the new database size you want, you must first prune your database using the `prune_asdb` command before you can reduce the database size.

See “prune_asdb” on page 114.

To change the maximum database size

1. From the Control Center, click **Administration**, then click **System Control**.
2. Under Database Size Limit, click on one of the three radio buttons.
3. Click **Resize**.

If the new maximum size is equal to or larger than the current actual database size, the maximum changes. If the new maximum size is smaller than the current actual database size, an error message appears.

Viewing the Changelog

Symantec Brightmail Traffic Shaper maintains an audit trail of manual changes made by all administrators in a change log. If you have System or Master Administrator privileges, you can view the audit trail.

The Changelog lists all changes made by Data and User Administrators using the Control Center as well as the time the change was made.

To view the Changelog

◆ In the Control Center, click **Administration**, then click on **Changelog**.
The Changelog page is displayed.

Administering user accounts

You can use the Control Center to set limits on the functions that specific users can perform by assigning them to administrative groups which have defined roles:

Group name	Access
Help Administrator	Can view the path data and standard reports.
Path Administrator	Can view and modify the path data and can also view standard reports.
Data Administrator	Can view and modify both the path data and the reports.
User Administrator	Can add, delete, and modify user accounts.
Master Administrator	Can perform any action, including changing configuration settings.
System Administrator	Can adjust the appliance state and power down the appliance.

To administer user accounts

- From the Control Center, click **Administration**, then click **User Administration** in the left menu.
  The User Administration page is displayed.

On this page, a set of tables display information about each user name, group and role defined in the system.

Changing a user password

The User Administration page lists each active user. You must first select a user before changing their credentials. You must have User Administrator privileges to change another user's password.

To change a user password

1. From the Control Center, click **Administration**, then click **User Administration** in the left menu.
   The User Administration page is displayed.
2. On the User Administration page, in the Users table, select the radio button next to the user name whose password you want to change and click **Edit.**
   The User Info page is displayed.
3. In the **Password** text box, type the new password.
4. In the **Confirm** text box, retype the new password.
5. Click **Apply Changes.**
   The password is changed.

Caution: Document the administrator password and store it in a safe place.The administrator password can not be reset if it is lost.

Adding a new user account

You must be a User Administrator or Master Administrator to add a new user account. Adding a new user account allows a that user to access the Control Center.

To add a new user account

1. From the Control Center, click **Administration**, then click **User Administration** in the left menu.
   The User Administration page is displayed.

2. At the bottom of the Users box, click **New User**.
   The New User page is displayed.
3. In the **User** name text box, type the user name of the new user.
4. In the **Password** text box, type a password for the new user.
5. In the **Confirm** text box, retype the password for the new user.

   Note: Under **Member Groups**, check the group(s) to which you want to assign the new user.

   Note: To define a read-only user, click **help admin** only.

6. Click **Apply Changes.**

Deleting a user account

Deleting a user's account means that they will no longer have access to the Control Center. You must be a Master or User Administrator to delete a user account.

Note: You cannot delete the Admin user account.

To delete a user account

1. In the Control Center, click **Administration**, then **User Administration**.
   The **User Administration** page is displayed.
2. In the **Users** box, select the checkbox next to the name of the user you wish to delete.
3. Click **Delete**.
4. Confirm the deletion.
   The user account is deleted.

Modifying an existing user account

Existing user accounts can be modified to change the group/role membership of the user or their password. You must be a Master or User Administrator to modify an existing user account.

To modify an existing user account

1. In the Control Center, click **Administration**, then **User Administration**.
   The User Administration page is displayed.
2. In the **Users** box, select the checkbox next to the name of the user you wish to modify.
3. Click **Edit**.
   The User page for this user is displayed.
4. If you want to change the user password,
   - In the **Password** text box, type the modified password of the user.
   - In the **Confirm** text box, type the modified password of the user.
5. If you want to change the groups to which this user belongs, under **Member Groups**, check the groups to which you want to assign the user.
6. Click **Apply Changes.**

Troubleshooting

The troubleshooting page allows you to test network connectivity to protected servers. Two tools are available, `ping` and `traceroute`. `ping` is most useful in virtual bridge mode or when Symantec Brightmail Traffic Shaper is acting as the router for the subnet on which the mail server(s) is located. `traceroute` is useful when the protected server is located behind another device such as a router.

Software updates from Symantec

You can view your current system software version and, if available, request software updates.

To view the current software version or request an update

1. In the Control Center, Select **Administration**, then click **Software Updates**.
   The newest version of the software, if newer than your installed version, appears.
2. If you wish to install new software, click **Install now**.
   The appliance will download the new software, update your existing installation, and then reboot. This may take a few minutes. During this time, you will not have access to the Control Center. When the system has rebooted, re-log into the Control Center and proceed.

Setting up alerts

You can specify up to 10 email addresses to which Symantec Brightmail Traffic Shaper will send alert notifications.The addresses you specify cannot be local to the appliance host.

Symantec Brightmail Traffic Shaper will send out the following alerts for the stated conditions:

- The appliance database is full; please prune the records.
  This alert is sent when the paths database reaches the maximum allowed number of records.
- The appliance database is no longer full.
  This alert is sent when the paths database was full but has been pruned.
- The appliance disk is at 90% capacity.
  This alert recommends that you use the CLI `clear` command to empty log files in order to recover disk space. Refer to "clear" on page 111 for information.
- The appliance has lost contact with other cluster member(s).
  This alert is sent when one or more of the connections to other appliance cluster members breaks off.
- The appliance has reestablished contact with other cluster member(s).
  This alert is sent when a previously broken connection to a cluster member is reestablished.
- A software upgrade is now available for installation.
  This alert is sent when a software upgrade is available for download/installation.

To specify email addresses to the alert list

1. From the Control Center, click **Settings**.
2. In the menu on the left, click **Edit Settings**, then click **Notification Management**.
   The Notification Management page is displayed.
3. Enter the email address to which you want the alerts to be sent.
   If there is more than one address, separate them with commas.
4. Enter the name of your SMTP server in the **SMTP Server** field.
5. If the SMTP server requires username and password, enter them in the **Account** and **Password** fields.
   The supported SMTP authentication method is CRAM_MD5.

6 Click **Send test email.**

7 Confirm with the recipient that the email was received. If the email was not received, adjust the settings on this page.

Managing Licenses

To view and add licenses

1 In the Control Center, Select **Administration**, then click **Licensing**.

2 Review the license information.

Next to each feature to which a license can apply, a start date and expiration date is shown.

3 To license a particular feature, either paste in a license key from an email you have received from Symantec, or browse for a filename in the Install a new license file box.

If you have licenses for other Symantec products in the same location, be sure you have selected the correct license before proceeding.

4 Click **Install**.

Appendix A

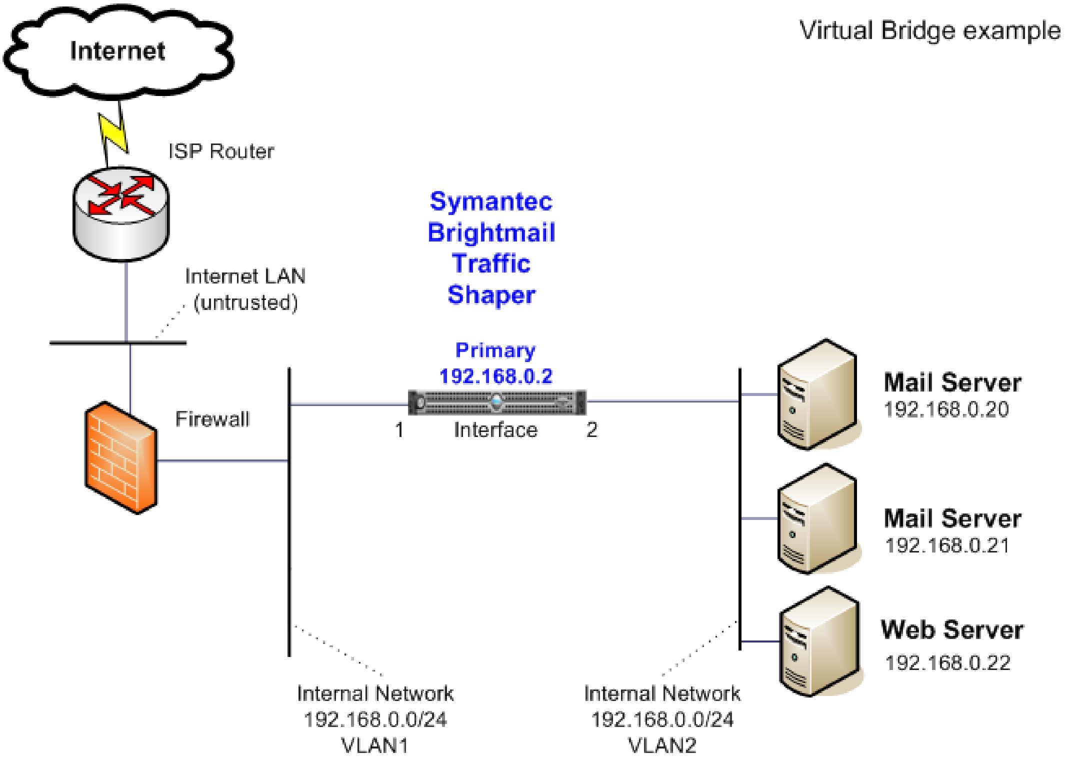
Example Deployment Scenarios

This Appendix contains examples of various potential deployment options for Symantec Brightmail Traffic Shaper, with information about how to implement Symantec Brightmail Traffic Shaper within the depicted network infrastructures.

High availability virtual bridge implementation

The diagram below shows an installation of two Symantec Brightmail Traffic Shaper appliances in virtual bridge mode, configured for high availability. In this configuration, the appliance designated as the primary appliance provides data synchronization to the secondary appliance. If the primary appliance is removed from service, the traffic flows to the secondary appliance, which has up-to-date configuration and path information. The instructions in "Setting up your appliance" on page 35 explain how to deploy two Symantec Brightmail Traffic Shaper appliances in this configuration.

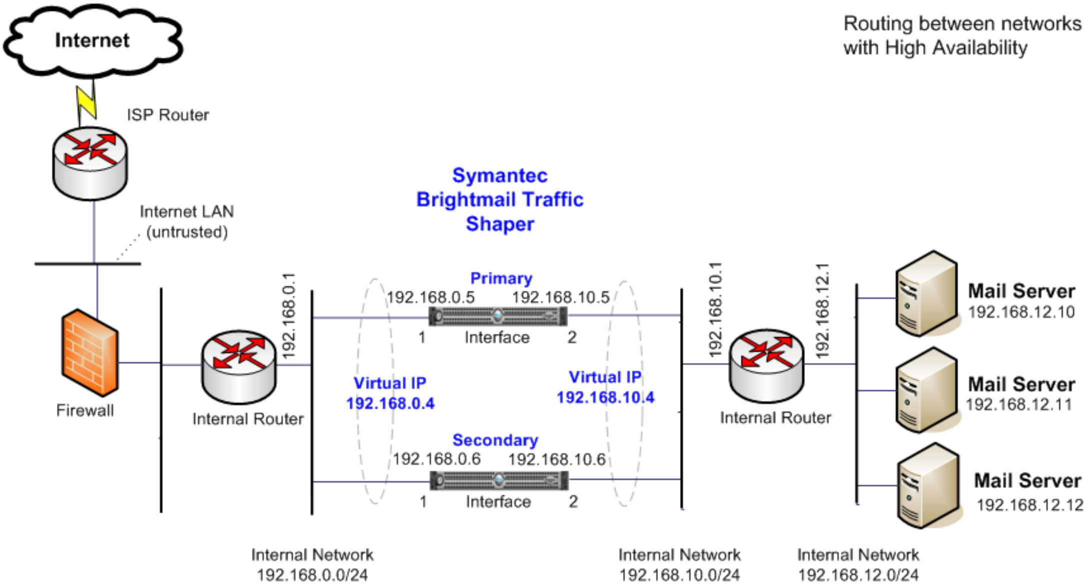
Figure A-1 Diagram of high availability virtual bridge mode configuration



High availability router implementation

The diagram below shows an installation of two Symantec Brightmail Traffic Shaper appliances in router mode, configured for high availability. In this configuration, the appliance designated as the primary appliance provides data synchronization to the secondary appliance. If the primary appliance is removed from service, the traffic flows to the secondary appliance, which has up-to-date configuration and path information. The instructions in "Setting up your appliance" on page 35 explain how to deploy two Symantec Brightmail Traffic Shaper appliances in this configuration.

Figure A-2 Diagram of high availability router mode implementation



In this example, mail from the "external network" is sent to 192.168.0.4.

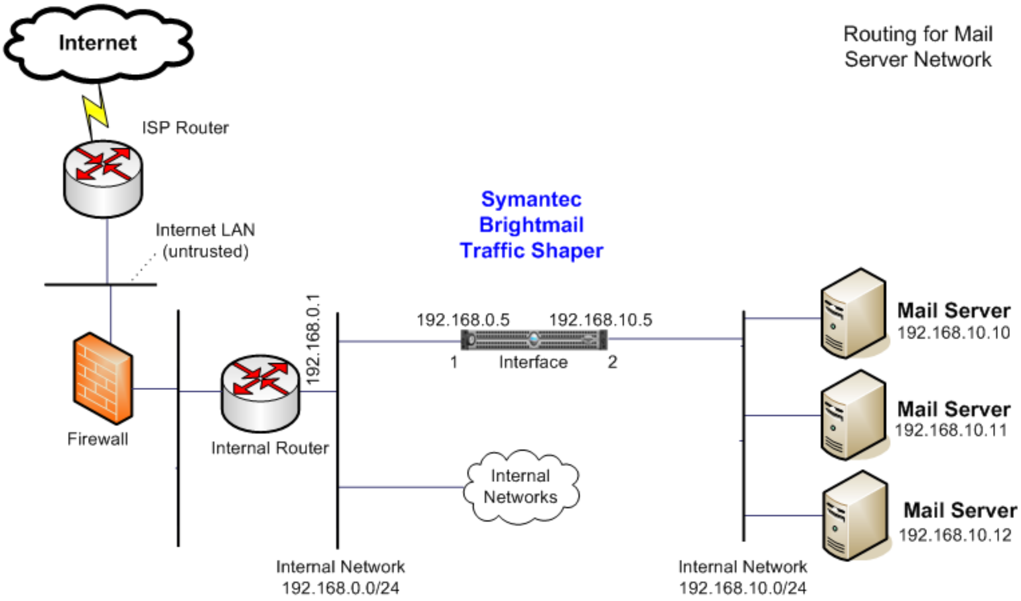
The next-hop gateway for the protected servers is 192.168.10.1.

The gateway for outbound traffic is 192.168.10.4.

Mail server gateway router implementation

In this implementation, your network is physically configured such that the only machines behind Symantec Brightmail Traffic Shaper appliances are SMTP servers. You can decrease traffic load on Symantec Brightmail Traffic Shaper by configuring your network this way.

Figure A-3 Diagram of high availability gateway router mode implementation



In this example, mail traffic from the "external network" is routed to 192.168.0.4.

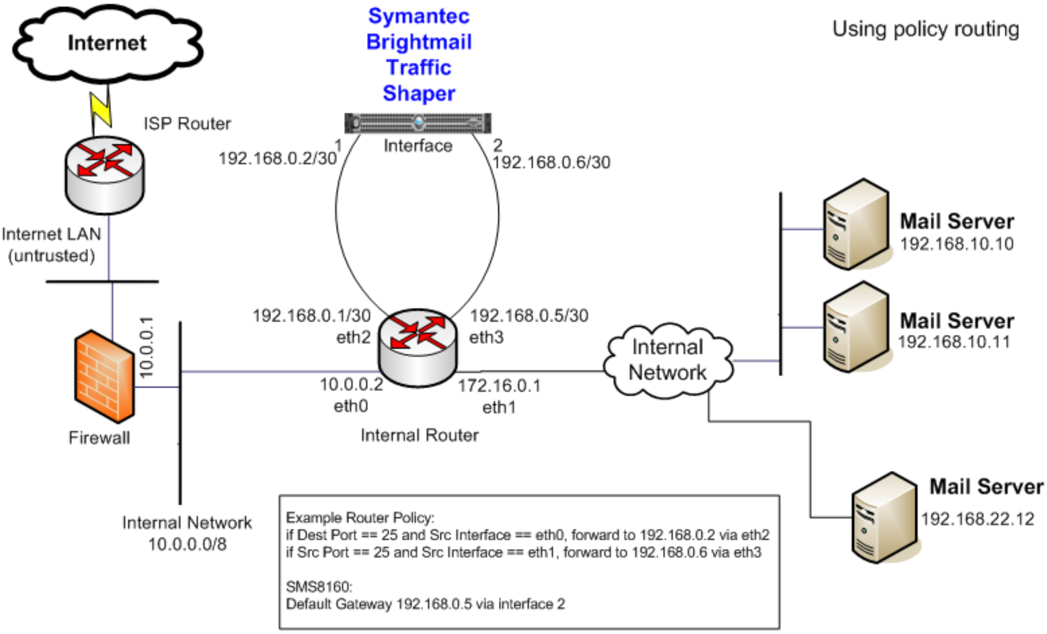
The next-hop gateway for the protected servers is 0.0.0.0.

The gateway for outbound traffic is 192.168.10.4.

Policy routed router implementation

In this implementation, only SMTP traffic flows through Symantec Brightmail Traffic Shaper. You accomplish this configuring your router to policy route only SMTP traffic through Symantec Brightmail Traffic Shaper. Return traffic must also be routed through the appliance. If your network carries a large amount of non-SMTP traffic and you cannot place the Symantec Brightmail Traffic Shaper appliances directly in front of the mail servers (as shown in "Mail server gateway router implementation" on page 106), you may wish to configure your Symantec Brightmail Traffic Shaper deployment this way to reduce traffic load on the appliances.

Figure A-4 Diagram of a policy routed implementation



```
Example Router Policy:
if Dest Port == 25 and Src Interface == eth0, forward to 192.168.0.2 via eth2
if Src Port == 25 and Src Interface == eth1, forward to 192.168.0.6 via eth3

SMS8160:
Default Gateway 192.168.0.5 via interface 2
```

To implement this configuration, set the default gateway on interface 2 rather than on the external interface 1 in step 11 in "To initialize your new appliance" on page 32.

Command Line Interface Reference

Each appliance has a set of commands you can use to configure, troubleshoot, and administer your system.

The following sections describe the commands available to you. To access these commands, you must open a shell session to Symantec Brightmail Traffic Shaper and log in as user **admin**. You can do this on the console, or remotely using ssh to port 22.

Caution: If you have more than one Symantec Brightmail Traffic Shaper deployed in a high availability configuration, make sure that any changes you make (for instance, using the `restore-config` command) take into account the configuration on other Symantec Brightmail Traffic Shaper appliances in your deployment.

asdbadmin

The `asdbadmin` command is used for remote automation of tasks manipulating the ASDB database of path information. You can pass `asdbadmin` a URL or a '-' (which indicates that the program will take its input from standard in).

The asdbadmin command has the following syntax:

```
asdbadmin <URI>
```

```
asdbadmin -
```

```
asdbadmin <FLAG> [ <PERCENT> ] [ <HOST> ]
```

Options

`<FLAG>` : Command to execute; refer to the Flags section below

`<HOST>` : IP address or fully-qualified domain name

`-` : Tell asdbadmin to read input from stdin

`<URI>` : URI pointing to an input file for asdbadmin (HTTP or HTTPS URIs only)

Flags

The command flags described here are distinct from the database flags reported by the ASDB database. In the example below, the `BRS` database flag represents the Brightmail Reputation Service.

The following flags are valid for use in commands passed to `asdbadmin`:

`WL <HOST>` : Mark the specified host as whitelisted

`BL <HOST>` : Mark the specified host as blacklisted

`DEL <HOST>` : Delete the record for the specified host

`SET <PERCENT> <HOST>` : Set the specified host's record to the specified spam percentage; `<PERCENT>` must be an integer in the range [0,100]

`SETLK <PERCENT> <HOST>` : Set the specified host's record to the specified spam percentage and lock it there, preventing the record's movement away from the specified score

`SETLK_TIMEOUT <PERCENT> <DAYS> <HOST>: S`et the specified host's record to the specified spam percentage and lock it there until the expiration <DAYS>, preventing the record's movement away from the specified score

`DELAA` : Delete all administratively-altered records from the ASDB

`SHOW <IP>` : Show the ASDB record for an IP address; `<IP>` must be in dotted quad format (*nnn.nnn.nnn.nnn*).

Sample output of the `SHOW` flag:

```
lastmodified=2008-05-15-T16:43:53 sampled=16 spam=72% flags=BRS
```

Note: Flags are case-insensitive.

Input Files

Input files are passed either via `stdin` or an HTTP or HTTPS URI. The file must be formatted in the following way:

- All commands must be specified on a line by themselves. Leading and trailing whitespace is ignored, as are any arguments after those required by the flag.
- A valid input file must be in 7-bit ASCII text format.

- A valid input file must end in the string "EOF" on a line by itself.

Note: You will likely not want to use the DELAA flag on anything other than the first line of the file.

Usage notes

When processing an input file, errors will be reported to the terminal but will not terminate further processing of the file.

The presence of EOF on the last line of the input file is the deciding factor when attempting to read an input file; if it is not present, no commands in the file are executed and the ASDB remains unchanged. Even when reading from stdin, asdbadmin will validate the presence of the EOF on a line by itself before performing any actions specified in the input. No actions specified after the EOF string will be acted upon.

bootstrap

The bootstrap command is run during the initial boot to configure the basic information on the appliance.

The bootstrap command has one optional switch, --reconfigure. Running bootstrap --reconfigure will erase the current configuration and allow you to start completely from scratch.

After running bootstrap –reconfigure, you must reinstall your license, and go through the Setup Wizard again.

After a configuration is activated, the bootstrap command exits immediately.

clear

The clear command clears all log files. You can use the clear command to free up disk space if you have received an alert message indicating that the appliance disk has reached 90% capacity.

gen_ssl_cert

Execute the gen_ssl_cert command when your appliance’s SSL certificate is about to expire (default: 1 year). This command will ask confirmation before generating a new SSL certificate and overwriting the old one. After the command completes, execute service httpd restart to load the new SSL certificate.

grep

The grep command searches within the system log files.

help

The help command displays a list of available commands on the appliance.

The help command has the following syntax:

```
help
```

ifconfig

The ifconfig command configures the network for an appliance. This command is part of the standard Linux command set. For additional details, try typing `ifconfig -?` or refer to a Linux user's manual of your choice. Note that changes to any network interfaces made with the ifconfig command will be lost the next time the system boots. For permanent changes, use the Site Setup Wizard in the Control Center.

iostat

The iostat command is used for monitoring system input/output device loading by observing the time the devices are active in relation to their average transfer rates.

The iostat command has the following syntax:

```
iostat <flags>
```

lcd

The lcd command is used to change the text that displays in the LCD window on the appliance.

By default, this display rotates between the following:

- SMS 8160
- hostname
- IP address of eth0

The lcd command has the following syntax:

- `lcd --set <text>`
- `lcd --get`
- `lcd --default`
- `lcd --disable`

<text> is the data to be displayed in the LCD window. When used with `set`, the `lcd` command changes the window display to the specified text.

When used with `get`, the `lcd` command displays the currently defined LCD window text.

When used with `default`, the `lcd` command restores the LCD window text to the default text.

When used with `disable`, the `lcd` command disables overwriting the BIOS LCD string on future reboots. This allows you to set the LCD string through the BIOS from the console.

netstat

The `netstat` command is used to print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. This command is part of the standard Linux command set. For additional details, try typing `netstat --help` or refer to a Linux user's manual of your choice.

The `netstat` command has the following syntax:

```
netstat <flags>
```

nslookup

The `nslookup` command performs a DNS lookup of the given hostname or IP address. This command is part of the standard Linux command set. For additional details, try typing `nslookup --help` or refer to a Linux user's manual of your choice.

The `nslookup command has the following syntax:`

```
nslookup <hostname|ip address>
```

outbound_cleanup

The `outbound_cleanup` command automatically purges the list of outbound IPs when Symantec Brightmail Traffic Shaper is operating in outbound protection mode. Running this command with the `-y` flag will erase all paths in the database listed in the Outbound Paths page. You can reach the Outbound Paths page from the Settings tab or the Paths tab.

passwd

The `passwd` command changes the password for the command line interface and Control Center login.

The passwd command has the following syntax:

```
passwd
```

ping

The ping command tests the transfer of data between the issuing machine and the given hostname or IP address. All arguments are permitted. This command is part of the standard Linux command set. For additional details, try typing ping --help or refer to a Linux user's manual of your choice.

The ping command has the following syntax:

```
ping <hostname|ip address>
```

prune_asdb

The prune_asdb command reduces the size of the database by deleting the oldest IP addresses. The prune_asdb command has the following syntax:

```
prune_asdb <size>
```

Options

<size>: Size of the database after the pruning operation is complete, as follows:

- A value of 10 results in a database size of 10 million (10,000,000) entries.
- A value of 20 results in a database size of 20 million (20,000,000) entries.
- A value of 50 results in a database size of 50 million (50,000,000) entries.
- If no value is specified, the current value for **Database Size Limit** on the **Administration > System Control** page is used.

reboot

The reboot command reboots the appliance and is part of the operating system.

The reboot command has the following syntax:

```
reboot
```

rebuildrpmdb

The rebuildrpmdb command recreates the RPM database for the appliance.

The rebuildrpmdb command has the following syntax:

```
rebuildrpmdb
```

remove-admin-files

The remove-admin-files command removes files from the /home/admin directory.

This command ignores the hidden .* files.

See "tcpdump" on page 122.

repupdate

The repupdate command can be remotely run to pipe in the contents of an xml file that meets specific requirements.

The repupdate command can be used for any of the following purposes:

- To remotely update the Symantec Brightmail Traffic Shaper database with spam scanning results from downstream mail security servers, for example from the Symantec Brightmail Message Filter.
- To remotely alter or delete a path from the Symantec Brightmail Traffic Shaper database.
- To remotely query the Symantec Brightmail Traffic Shaper database.

The repupdate command must be run from a remote server with the following syntax:

```
cat <file.xml> | ssh admin@<ip address|hostname> repupdate >
output.xml
```

<file.xml> is the filename for your data input file that meets the requirements.

<ip address|hostname> is a pointer to your Symantec Brightmail Traffic Shaper.

Input file requirements and output formats

Within input files, carriage returns (CR), line feeds (LF), and spaces are allowed within tags that can enclose other tags. However, within tags that enclose one piece of data only, such as an IP address, spaces are not allowed. Table B-1 describes the xml tags used in the input and output files, and indicates the input tags that do not allow spaces.

Table B-1 XML tags for repUpdate command input and output files

Tag	Description
repData	The repData tag denotes the beginning and end of the data for the **repUpdate** command to process.
queryCmd	The query command requests data from the database.

Table B-1 XML tags for repUpdate command input and output files

Tag	Description
`path`	The `path` command specifies an IP address, CIDR range, or domain for a query. Spaces are not allowed.
`queryResponse`	The `queryResponse` tag denotes the beginning and end of the data output in response to a query.
`ret`	For any kind of output, the return tag indicates if processing was successful or failed.
`err`	For any kind of output, the error tag can include an error message.
`out`	For any kind of output, the output tag denotes the beginning and end of the output data. The `out` tag can include one or more `row` tags.
`row`	For any kind of output or input, the `row` tag denotes the start and end of one set of data.
`ip`	The `ip` tag encloses an IP address, and in some cases a CIDR range or domain. Spaces are not allowed.
`msgs`	The messages tag encloses a number that indicates the number of messages allowed or reported for a sender. Spaces are not allowed.
`spm`	The spam tag encloses a number that indicates the number of spam messages allowed or reported for a sender. Spaces are not allowed.
`lck`	The lock tag indicates that a path is locked. The lock ensures that the path stays in the bucket indicated by the `bkt` tag, for the number of days indicated by the `exp` tag.
`bkt`	The bucket tag indicates the bucket in which a path is locked. Spaces are not allowed.
`exp`	The expiry tag indicates the number of days for which a path is locked. You can specify any integer from 1 to 999, inclusive. Spaces are not allowed.
`bl`	The blacklist tag encloses either true or false to indicate whether the sender is/should be blacklisted. Spaces are not allowed.
`wl`	The whitelist tag encloses either true or false to indicate whether the sender is/should be whitelisted. Spaces are not allowed.

Table B-1 XML tags for repUpdate command input and output files

Tag	Description
`src`	The source tag indicates the source of the information for the output, either: ■ BRS (Brightmail Reputation Service, aka Global Intelligence Network) ■ BEIK (Brightmail Engine Installation Kit)? Spaces are not allowed.
`mod`	In output, the modified tag shows that date on which a path was last modified.
`updateCmd`	For an update, the `updateCmd` tag encloses the input data. The `updateCmd` tag can include one or more `row` tags.
`ipList`	For an update, the `ipList` tag encloses a list of IP addresses.
`act`	For an update, the `act` tag encloses the action to be taken on a sender or group of senders.
`rem`	For an update, the remove tag indicates whether or not (true or false) a sender should be removed from the database. Spaces are not allowed.
`updateResponse`	For an update, the `updateResponse` tag encloses the output data.

For queries, the input file must have the following form:

```
<repData>
        <queryCmd>
                <path>IP address/CIDR/Domain</path>
        <queryCmd>
</repData>
```

The tags above are required. If the path tag is empty, an error returns.

The query output is in the following form:

```
<repData>
        <queryResponse>
        <ret>success/fail</ret>
        <err>message</err>
        <out>
              <row>
                    <ip>IP address</ip>
                    <msgs>number of messages</msgs>
                    <spm>number of spam messages</spm>
                    <lck>
                          <bkt>bucket number</bkt>
                          <exp>date</exp>
                    </lck>
```

```
                   <bl>true/false</bl>
                   <wl>true/false</wl>
                   <src>BRS/BEIK</src>
                   <mod>date</mod>
             </row>
        </out>
        </queryResponse>
</repData>
```

For an update or database change, the input file must have the following form:

```
<repData>
        <updateCmd>
           <row>
                 <ipList>
                     <ip>IP address/CIDR</ip>
                     <ip>IP address/CIDR</ip>
                 </ipList>
                 <act>
                       <msgs>number of messages</msgs>
                       <spm>number of spam messages</spm>
                       <lck>
                            <bkt>bucket number</bkt>
                            <exp>number of days</exp>
                       </lck>
                       <bl>true/false</bl>
                       <wl>true/false</wl>
                       <rem>true/false</rem>
                 </act>
           </row>
        </updateCmd>
</repData>
```

The `updateCmd` tag is required with at least one `row` tag. Each `row` tag must have one `ipList` tag and one act tag that specifies the action required. An `ipList` tag can have as many `ip` tags as needed.

The `act` tag should have tags that implement specific action. For example, to blacklist IP address 0.0.0.0, the command is:

```
<repData>
        <updateCmd>
             <row>
               <ipLst>
                     <ip>0.0.0.0.</ip>
               </ipList>
               <act>
                       <bl>true</bl>
               </act>
             </row>
        </updateCmd>
<repData>
```

The update command output is in the following format:

```
<repData>
         <updateResponse>
         <ret>success/fail</ret>
         <err>erorr message</err>
         <out></out>
         </updateResponse>
</repData>
```

restore-config

The `restore-config` command reverts from the current version to the last saved version. It takes no arguments.

route

The `route` command allows for the viewing and manipulation of the IP routing table. Its primary use is to set up static routes to specific hosts or networks via interface, after it has been configured with the `ifconfig` command.

service

The `service` command allows for the changing of status for components within the appliance.

The `service` command has the following syntax:

```
service <component_name> <command>
```

where:

- component_name can be any one of the following:
    - asrctl - the Symantec Brightmail Traffic Shaper software
    - asrconfig - the Symantec Brightmail Traffic Shaper configuration
    - httpd - the httpd service (so you can restart the httpd service after regenerating your SSL certificate)
    - osconfig - OS-level configuration
    - stunnel - the secure (SSL) connection
- command can be any one of the following:
    - start
    - stop
    - restart

servicetag

The `servicetag` command displays the appliance service tag.

showarp

The `showarp` command displays the ARP table on the appliance.

The `showarp` command has the following syntax:

```
showarp
```

shutdown

The `shutdown` command shuts down the appliance.

The `shutdown` command has the following syntax:

```
shutdown
```

ssh-key

The `ssh-key` command has the following syntax:

- `ssh-key <show|delete|contents of public key file>`

With the `show` argument specified, the ssh-key command displays the current contents of the `/home/admin/.ssh/authorized_keys` file.

With the `delete` argument specified, the `ssh-key` command removes any `/home/admin/.ssh/authorized_keys` existing file.

With any other text specified, the `ssh-keys` command writes the specified text to the `/home/admin/.ssh/authorized_keys` file.

By installing an ssh key, you can log in as admin user using an authentication mechanism other than a password. By using an ssh key with no passphrase, you can remotely run commands on your appliance from an automated script that you control.

For example:

- `ssh admin@`*host command arguments*

stagectl

The `stagectl` command lets you change the traffic control settings by switching to Passthrough, any of the five pre-configured stages, or any saved custom stages.

- `--list`—lists all of the stage names, including passthrough and custom stages
- `--change<stagename>`—changes the stage to the new stage
- `--help`— provides usage information

- `--current`—provides the current stage
- `--details<stagename>`— provides a table output of detail of the selected stage

systemname

The `systemname` command returns the appliance system name.

system-stats

The `system-stats` command is used to display system statistics.

The `system-stats` command has the following syntax:

```
system-stats <key>
```

where `key` can be blank, in which case all available values are returned, or one or more of the following:

- `cpu_usage`—Displays the CPU usage as a percentage
- `disk_used`—Displays the disk used in KB
- `disk_free`—Displays the disk free in KB
- `mem_used`—Displays the memory used in KB
- `mem_free`—Displays the memory free in KB
- `swap_used`—Displays the amount of swap in use
- `swap_free`—Displays the amount of free swap
- `eth0_in`—Displays the current incoming data rate in KB
- `eth0_out`—Displays the current outgoing data rate in KB
- `eth1_in`—Displays the current incoming data rate in KB
- `eth1_out`—Displays the current outgoing data rate in KB
- `disk_in`—Displays the current rate of disk writes in KB
- `disk_out`—Displays the current rate of disk reads in KB

tail

The `tail` command shows the last 50 lines of the `/data/logs/messages` log file. It takes no arguments.

tcpdump

If you are logged in with `sudo` privileges as the user `admin`, you can run the `tcpdump` command to troubleshoot traffic flow on the appliance. Be sure to specify an appropriate filter when running `tcpdump`. Here is an example of a filter that will only dump packets from the specified IP address:

```
tcpdump src host nnn.nnn.nnn.nnn
```

Usage of `tcpdump` will negatively impact performance on systems under heavy load.

See "remove-admin-files" on page 115.

traceroute

The `traceroute` command traces the network route to the given hostname or IP address and is part of the operating system. All arguments are permitted. This command is part of the standard Linux command set. For additional details, type `traceroute --help` or refer to a Linux user's manual of your choice.

The `traceroute` command has the following syntax:

```
traceroute <hostname|ip address>
```

```
update
```

```
The update command can check for new packages, download new
packages, install new packages on the appliance, and list available
versions for installation.
```

```
The update command has the following syntax:
```

update <option>

where *option* can be any of the following:

- `check`—compares installed and available packages to check whether or not your installation is current.
- `download`—Fetches any new packages for future installation.
- `install`—Installs the most recent packages to your appliance.
- `list`—Displays a list of installations available on your appliance.

userlist

The `userlist` command is designed to be run remotely over ssh, and has two variants:

- `userlist-get`—prints to standard output the current contents of the Web user interface password file in uuencoded format, plus a checksum.
- `userlist-set`—reads from standard input data. The data must be in the format produced by running `userlist-get`, complete with checksum at the end. If the data is in the correct format and the checksum is correct, `userlist-set` overwrites the Web user interface password file with the supplied contents.

For example, if you have four appliances, you could execute the following commands to copy the Web user interface password file from the first appliance to the other three appliances:

```
ssh admin@asr01 userlist-get > userlist
ssh admin@asr02 userlist-set < userlist
ssh admin@asr03 userlist-set < userlist
ssh admin@asr04 userlist-set < userlist
```

version

The `version` command displays the version of software being run by the appliance.

The `version` command has the following syntax:

```
version
```

watch

The `watch` command executes `tail -f /data/logs/messages`, sending output to the screen for monitoring.

watchmarks

The `watchmarks` command prints the current bucket utilization details.

The `watchmarks` command has the following syntax:

- watchmarks [-v] [-n <seconds>]

With the `-v` argument specified, the `watchmarks` command will also print the system statistics.

With the `-n` argument specified, the `watchmarks` command will print every n seconds. If `-n` is not specified, the default behavior is to print every second.

Appendix C

SNMP MIB Reference

This appendix contains the MIB for Symantec Brightmail Traffic Shaper. You can also download the MIB from Symantec from the Notification Management panel under the Settings tab. For information about configuring SNMP for Symantec Brightmail Traffic Shaper, refer to “To set up notifications” on page 45.

```
---------------------------------------------------------------------------------------------------
SYMANTEC-SMTP-TRAFFIC-SHAPING DEFINITIONS ::= BEGIN

IMPORTS
  NOTIFICATION-GROUP
    FROM SNMPv2-CONF
  MODULE-IDENTITY,
  OBJECT-TYPE,
  NOTIFICATION-TYPE,
  Counter32,
  Gauge32,
  Counter64,
  Unsigned32,
  enterprises
    FROM SNMPv2-SMI
  DisplayString
    FROM SNMPv2-TC;

symantecOBJECT IDENTIFIER ::= { enterprises 393 }
productsOBJECT IDENTIFIER ::= { symantec 200 }
sms OBJECT IDENTIFIER ::= { products 130 }
```

```
symantecSMTPTrafficShaping MODULE-IDENTITY
  LAST-UPDATED"200505261709Z"
  ORGANIZATION"Symantec Corporation"
  CONTACT-INFO
    "   Symantec Corporation
        20300 Stevens Creek Blvd.
        Cupertino, CA 95014
        US

        408-517-8000"
  DESCRIPTION
    "The MIB module to describe statistics and traps that apply
    to the Symantec SMTP Traffic Shaping capabilities."
  REVISION"200505261709Z"
  DESCRIPTION
    "Initial revision."
  ::= { sms 1 }

sstsPathCount OBJECT-TYPE
  SYNTAXGauge32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The number of known paths in the SMTP Path database."
  ::= { symantecSMTPTrafficShaping 1 }

sstsBlocklistRejected OBJECT-TYPE
  SYNTAXCounter64
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The number of times that connections were rejected due to
    the source path being listed as blocked."
  ::= { symantecSMTPTrafficShaping 2 }

sstsStageName OBJECT-TYPE
  SYNTAXDisplayString (SIZE (0..255))
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The name of the current stage of SMTP resource management."
  ::= { symantecSMTPTrafficShaping 3 }

sstsClassNumber OBJECT-TYPE
  SYNTAXUnsigned32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The number of SMTP classes present on this system."
  ::= { symantecSMTPTrafficShaping 4 }

sstsStatsTable OBJECT-TYPE
  SYNTAXSEQUENCE OF SstsClassStats
  MAX-ACCESSnot-accessible
  STATUScurrent
  DESCRIPTION
    "A list of SMTP class entries. The number of entries is given
    by the value of sstsClassNumber."
  ::= { symantecSMTPTrafficShaping 5 }

sstsClassStats OBJECT-TYPE
  SYNTAXSstsClassStats
  MAX-ACCESSnot-accessible
  STATUScurrent
  DESCRIPTION
    "An entry describing the accrued statistics pertaining to a
    given SMTP class."
  INDEX{ sstsClassStatsIndex }
  ::= { sstsStatsTable 1 }

SstsClassStats ::=
  SEQUENCE {
    sstsClassStatsIndexInteger32,
    sstsClassStatsNameDisplayString,
    sstsClassStatsConnectionLoadGauge32,
    sstsClassStatsConnectionAttemptsCounter64,
    sstsClassStatsConnectionAcceptedCounter64,
    sstsClassStatsMessagesCounter64,
    sstsClassStatsRecipientsCounter64
  }

sstsClassStatsIndex OBJECT-TYPE
  SYNTAXInteger32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The index for this row of the table."
  ::= { sstsClassStats 1 }

sstsClassStatsName OBJECT-TYPE
  SYNTAXDisplayString (SIZE (0..255))
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The name of this SMTP class, indicating the spam percentage
    that a path must have for its connections to be members of
    this class."
  ::= { sstsClassStats 2 }

sstsClassStatsConnectionLoad OBJECT-TYPE
  SYNTAXGauge32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The number of active connections currently attributed to this
    SMTP class."
  ::= { sstsClassStats 3 }

sstsClassStatsConnectionAttempts OBJECT-TYPE
  SYNTAXCounter64
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The number of connection attempts that have been made for this
    SMTP class."
  ::= { sstsClassStats 4 }

sstsClassStatsConnectionAccepted OBJECT-TYPE
  SYNTAXCounter64
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The number of connection attempts that have been accepted into
    this SMTP class."
  ::= { sstsClassStats 5 }

sstsClassStatsMessages OBJECT-TYPE
  SYNTAXCounter64
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The number of messages that have been sent by connections
    in this SMTP class."
  ::= { sstsClassStats 6 }

sstsClassStatsRecipients OBJECT-TYPE
  SYNTAXCounter64
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The number of message recipients that have been seen in
    messages in this SMTP class."
  ::= { sstsClassStats 7 }

sstsConfigTable OBJECT-TYPE
  SYNTAXSEQUENCE OF SstsClassConfig
  MAX-ACCESSnot-accessible
  STATUScurrent
  DESCRIPTION
    "A list of SMTP class entries. The number of entries is given
    by the value of sstsClassNumber."
  ::= { symantecSMTPTrafficShaping 6 }

sstsClassConfig OBJECT-TYPE
  SYNTAXSstsClassConfig
  MAX-ACCESSnot-accessible
  STATUScurrent
  DESCRIPTION
    "An entry describing the configuration pertaining to a given
    SMTP class."
  INDEX{ sstsClassConfigIndex }
  ::= { sstsConfigTable 1 }

SstsClassConfig ::=
  SEQUENCE {
    sstsClassConfigIndexInteger32,
    sstsClassConfigNameDisplayString,
    sstsClassConfigBandwidthUnsigned32,
    sstsClassConfigConnectionLimitUnsigned32,
    sstsClassConfigSpamLimitUnsigned32,
    sstsClassConfigConnectionsPerPathLimitUnsigned32,
    sstsClassConfigMessagesPerConnectionLimitUnsigned32,
    sstsClassConfigReconnectTimeoutUnsigned32
  }

sstsClassConfigIndex OBJECT-TYPE
  SYNTAXInteger32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The index of this row in the table."
  ::= { sstsClassConfig 1 }

sstsClassConfigName OBJECT-TYPE
  SYNTAXDisplayString (SIZE (0..255))
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The name of this SMTP class, indicating the spam percentage
    that a path must have for its connections to be members of
    this class."
  ::= { sstsClassConfig 2 }

sstsClassConfigBandwidth OBJECT-TYPE
  SYNTAXUnsigned32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The amount of bandwidth allotted to all connections in this
    SMTP class. Each connection will receive a fraction of the
    bandwidth proportional to the total bandwidth divided by the
    limit of connections in this class."
  ::= { sstsClassConfig 3 }

sstsClassConfigConnectionLimit OBJECT-TYPE
  SYNTAXUnsigned32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The total number of connections that will be allowed to
    simultaneously exist from paths that fall in this class.
    Connection attempts happening after this limit is reached
    will fall into worse SMTP classes or be rejected if those
    are also full."
  ::= { sstsClassConfig 4 }

sstsClassConfigSpamLimit OBJECT-TYPE
  SYNTAXUnsigned32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The limit on the percentage of spam sent that a path could
    have recorded in the database such that it would still be
    classified in this SMTP class."
  ::= { sstsClassConfig 5 }

sstsClassConfigConnectionsPerPathLimit OBJECT-TYPE
  SYNTAXUnsigned32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The limit on the number of concurrent connections that a
    single path could have open."
  ::= { sstsClassConfig 6 }

sstsClassConfigMessagesPerConnectionLimit OBJECT-TYPE
  SYNTAXUnsigned32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The limit on the number of messages that a path could send
    during the course of a single connection."
  ::= { sstsClassConfig 7 }

sstsClassConfigReconnectTimeout OBJECT-TYPE
  SYNTAXUnsigned32
  MAX-ACCESSread-only
  STATUScurrent
  DESCRIPTION
    "The number of seconds that a path would have to wait before
    it could reconnect after meeting its ConnectionsPerPathLimit.
    Connection attempts before this timeout expires will be
    rejected. This timeout is applied from the beginning of the
    connection."
  ::= { sstsClassConfig 8 }

sstsDatabaseFull NOTIFICATION-TYPE
  OBJECTS{ sstsPathCount }
  STATUScurrent
  DESCRIPTION
    "This trap indicates that the SNMP agent has detected that
    the SMTP Path Database is filled to capacity and can no
    longer sustain additional insertions."
  ::= { symantecSMTPTrafficShaping 7 }

sstsDatabaseNotFull NOTIFICATION-TYPE
  OBJECTS{ sstsPathCount }
  STATUScurrent
  DESCRIPTION
    "This trap indicates that the SNMP agent has detected that
    the SMTP Path Database is no longer filled to capacity and
    can now sustain insertions. This will be fired when the
    Database becomes not full after it had previously been full."
  ::= { symantecSMTPTrafficShaping 8 }

sstsDatabaseFullNotFullNotificationGroup NOTIFICATION-GROUP
  NOTIFICATIONS{ sstsDatabaseFull, sstsDatabaseNotFull }
  STATUScurrent
  DESCRIPTION
    "The notifications which indicate specific changes in
    sstsPathCount."
  ::= { symantecSMTPTrafficShaping 9 }

END
```

Index